2016-1046, -1048

United States Court of Appeals for the Federal Circuit

DATATREASURY CORPORATION,

Appellant,

v.

FIDELITY NATIONAL INFORMATION SERVICES, INC.,

Appellee.

Appeals from the United States Patent and Trade-mark Office, Patent Trial and Appeal Board in Nos. CBM2014-00020 and CBM2014-00021.

BRIEF FOR APPELLANT

DEREK T. GILLILAND
NIX PATTERSON & ROACH, LLP
205 Linda Drive
Daingerfield, TX 75638
(903) 645-7333
dgilliland@nixlawfirm.com

EDWARD K. CHIN
CHRISTIAN JOHN HURT
NIX PATTERSON & ROACH, LLP
5215 N. O'Connor Boulevard
Suite 1900
Irving, TX 75039
(972) 831-1188
edchin@me.com
christianhurt@nixlawfirm.com

Counsel for Appellant

JANUARY 6, 2016

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

DataTreasury Corporation v. Fidelity National Information Services, Inc.

No. 2016-1046; - 1048

CERTIFICATE OF INTEREST

Counsel for Appellant, Christian Hurt, certifies the following:

1. The full name of every party or amicus represented by me is:

   DataTreasury Corp.

2. The name of the real party in interest (if the party named in the caption is not the real party in interest) represented by me is:

   None.

3. All parent corporations and any publicly held companies that own 10 percent or more of the stock of the party or amicus curiae represented by me are:

   None.

4. The names of all law firms and partners or associates that appeared for the party or amicus now represented by me in the trial court or agency or are expected to appear in this court are:

   Abraham Hershovitz; Eugene C. Rzucidlo, Hershkovitz & Associates, PLLC.

   The names of all law firms and partners or associates that appeared for the party or amicus now represented by me in co-pending trial court litigation involving the patents subject to this appeal are:

   Nix Patterson & Roach, LLP; Nelson James Roach; Derek Tod Gilliland; Andrew Joseph Wright (former); Christian J. Hurt; Edward K Chin; Kirk Austin Voss; Robert Winn Cutler; Ross Leonoudakis; Ben King

   Kendall Law Group, LLP; Elton Joe Kendall; Karl A. Rupp

Albritton Law Firm; Eric M Albritton

Ward, Smith & Hill, PPLC; Thomas John Ward, Jr.

DATED: January 6, 2016.

Respectfully submitted,

/s/ Christian Hurt

CHRISTIAN HURT
Attorney for Appellant

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes & Rules

Other Authority

STATEMENT OF RELATED CASES

There are a number of related proceedings pending before this Court involving proceedings from the Patent Trial & Appeal Board ("Board") with regard to the same two patents: U.S. Patent No. 5,910,988 ("the '988 Patent") and U.S. Patent No. 6,032,137 ("the '137 Patent") (collectively, "the Patents"). Specifically, the Court has deemed related to this consolidated appeal the following pending appeals: *DataTreasury Corp. v. Jack Henry & Assoc., Inc.*, Case Nos. 16-1050, -1052; *DataTreasury Corp. v. Fiserv, Inc.*, Case Nos. 16-1229, -1230; and *In re DataTreasury Corp.*, Case No. 16-1250.

In addition, Appellant DataTreasury Corporation ("DataTreasury") has asserted infringement of the '988 and '137 Patents in the following actions pending in the U.S. District Court for the Eastern District of Texas: *DataTreasury Corp. v. Fiserv, Inc.*, Case No. 2:13-CV-00431-JRG-RSP, *DataTreasury Corp. v. Fidelity Nat'l Information Servs., Inc.*, Case No. 2:13-CV-00432-JRG-RSP, and *DataTreasury Corp. v. Jack Henry & Assoc., Inc.*, Case No. 2:13-CV-00433-JRG-RSP. Those actions are presently stayed.

JURISDICTIONAL STATEMENT

This consolidated appeal arises from two covered business method review ("CBM") proceedings under § 18 of the Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284 (2011). Under Section 18(a)(1) of the

AIA, CBM proceedings "shall be regarded as, and shall employ the standards and procedures of, a post-grant review under chapter 32 of title 35, United States Code," subject to some exceptions. The Board concluded it had the power to institute CBM proceedings, issued a final written decision, and denied DataTreasury's requests for rehearing. This Court thus has jurisdiction under 28 U.S.C. § 1295(a)(4)(A).

STATEMENT OF THE ISSUES

This appeal presents three issues: (1) whether the Board correctly concluded that the Patents are eligible for CBM review, even though they claim technological components combined in a novel and non-obvious manner; (2) whether the Board correctly concluded that all of the claims of the Patents fail to claim patent-eligible subject matter based on an analysis of two claims, even though the claims are directed to a specific network computer system that operates in a specific manner; and (3) whether the Board correctly found that the Patents do not adequately describe encryption of "subsystem identification information," even though the Patents specifically disclose encryption of bitmap image data where the image data can include "subsystem identification information."

STATEMENT OF THE CASE

This appeal challenges the PTAB's Final Written Decisions and Decisions on DataTreasury's Requests for Rehearing. Joint Appendix ("J.A.") 1–8,

Rehearing Decision for the ’137 Patent; J.A. 9–33, Final Written Decision for the ’137 Patent; J.A. 84–91, Rehearing Decision for the ’988 Patent; J.A. 92–114, Final Written Decision for the ’988 Patent. In particular, DataTreasury challenges the Board’s determination that the Patents are subject to CBM Review, the Board’s conclusion that every claim of the Patents is not directed to patent-eligible subject matter, and the Board’s finding that claims 1–67 of the ’137 Patent and claims 1–41 and 51–69 of the ’988 Patent lack written description support.

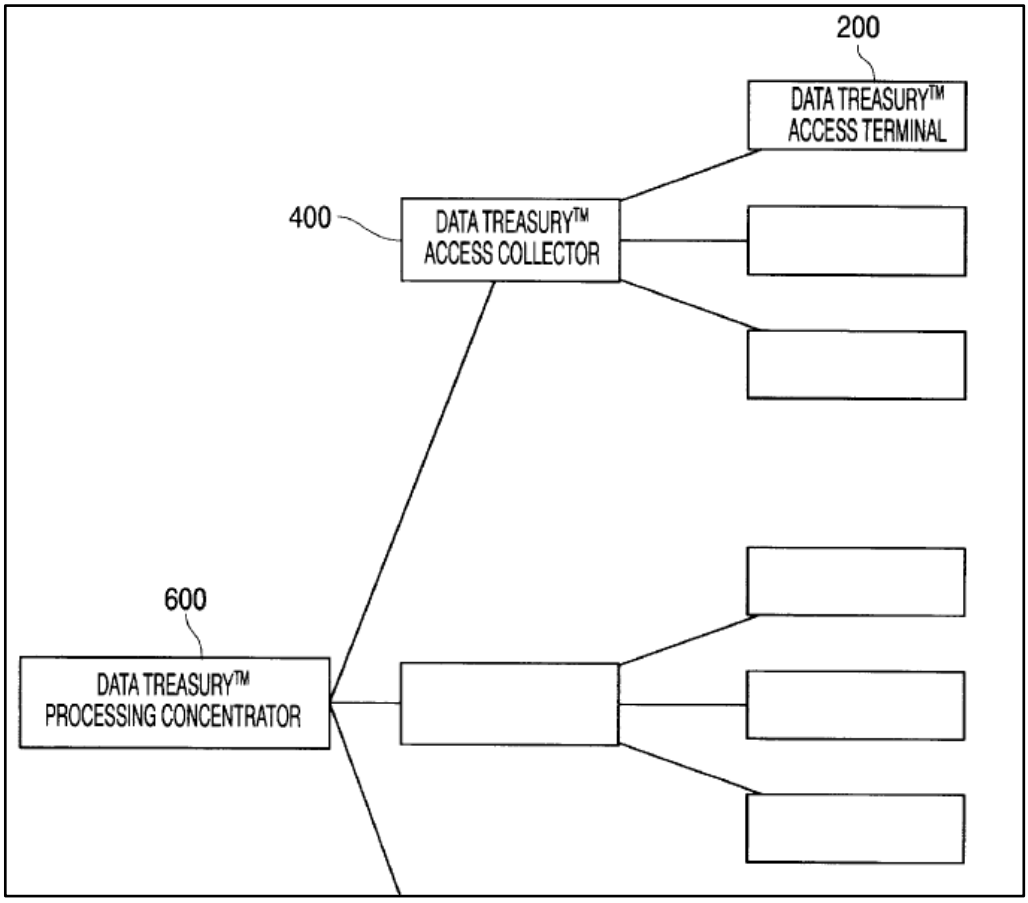
STATEMENT OF THE FACTS

I. The Technology of the ’988 and ’137 Patents

The Patents relate to a multi-tiered networked computer system used to capture, process, transmit, and encrypt data collected from a document, such as a receipt image or a check image.[1] The specification discloses a three-tier system, with a computer system at each tier. The top-tier is what the Patents refer to as the DataTreasury™ Processing Concentrator (“DPC”). J.A. 141, ’988 Patent, Fig. 1. Below that tier is a tier of DataTreasury™ Access Collector (“DAC”) computer systems distributed in a number of regions. *Id.* Both the DPC and the DAC are driven by servers, such as Windows-based servers. J.A. 156, ’988 Patent, col. 11

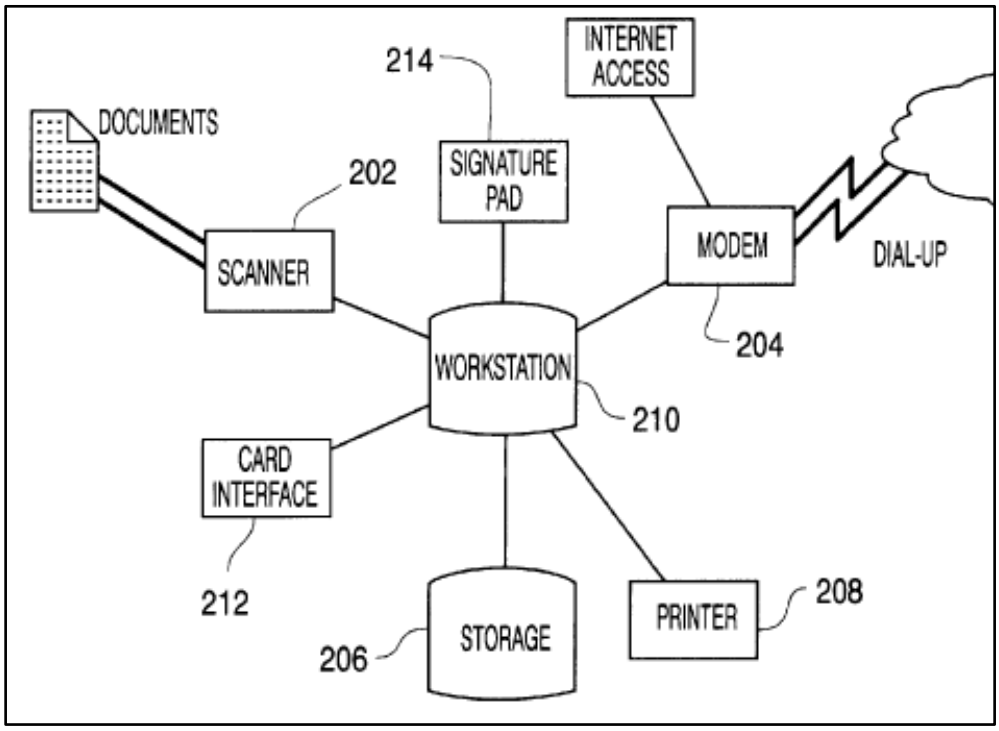
[1] The ’137 Patent is a continuation-in-part of the ’988 Patent but contains some additional matter. Thus, for ease of reference, this brief will generally cite to the specification of the ’988 Patent.

ll. 12–43; J.A. 157, '988 Patent, col. 14 ll. 19–33. Lastly, under the DAC tier is a tier of DataTreasury™ Access Terminal ("DAT") computer systems, which are remote terminals. The DAT is workstation-based computer system. J.A. 153, '988 Patent, col. 5 ll. 26–38. The multi-tiered structure of the system is shown below.



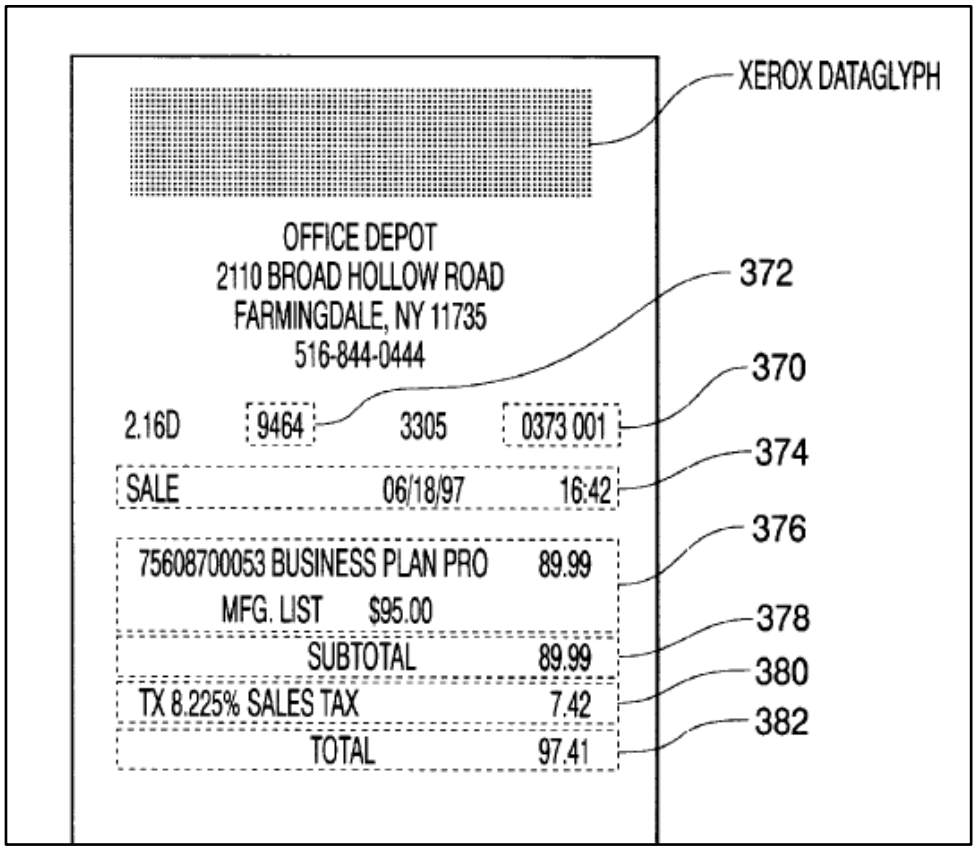
J.A. 141, '988 Patent, Fig. 1.

The system generally captures, encrypts, and transmits two pieces of digital data—transaction data and identification data. The process begins at the DAT, which is depicted below.



J.A. 142, '988 Patent, Fig. 2.

The DAT scanner (202) scans a document, such as a receipt, and reads data from the document. J.A. 153, '988 Patent, col. 5 ll. 46–57. The DAT can read images, text, and other data, such as the bits represented by a DataGlyph™. J.A. 153, '988 Patent, col. 5 l. 58–col. 6 l. 6. The DAT converts the document into a bitmap image. J.A. 153, '988 Patent, col. 5 ll. 46–57. A portion of an exemplary image of a receipt is shown below.



J.A. 144, '988 Patent, Fig. 3B

The exemplary receipt contains two sets of data (1) transaction information, such as the item purchased or its price (labeled 376); and (2) identification information, such as the identifier of the credit card terminal used to print the receipt (labeled 372). Though not specifically depicted in the exemplary receipt in Figure 3B, the Patents teach that the receipt can contain "appropriate identification information such as the transaction amount, the customer, the DAT 200, the transaction date, the transaction tax, the credit card number, the credit card expiration date, etc." J.A. 155, '988 Patent, col. 10 ll. 61–67. The "DAT 200" is

the identification information for the DAT terminal associated with the scanning of the image. J.A. 155, '988 Patent, col. 10 ll. 31–33.

The DAT controller (labeled WORKSTATION 210 in Figure 2) then encrypts the data received from the document. J.A. 154, '988 Patent, col. 7 ll. 31–40. In the bitmap image embodiment, the DAT controller compresses, encrypts, and tags the bitmap image data. J.A. 154, '988 Patent, col. 7 ll. 31–40, col. 7 l. 51–col. 8 l. 22. The DAT can store that data and, over the network, when polled, transmit the encrypted data and the tag to the DAC in the hierarchy. J.A. 154, '988 Patent, col. 7 ll. 41–51.

The DAC first polls each DAT in its region. J.A. 146, '988 Patent, Fig. 5; J.A. 157, '988 Patent, col. 13 l. 16–col. 14 l. 18. If the DAT contains additional encrypted data and tags, it transmits that data to the DAC. *Id.* The DAC then stores the encrypted data and tags. *Id.* A core concern of the system is security, J.A. 152, '988 Patent, col. 3 ll. 26–29, and the communications between the DAT and DAC can occur on an open communications channel (such as a carrier cloud). As a result, the DataTreasury system employs encryption to secure the communications. *See* J.A. 153–54, '988 Patent, col. 6 ll. 3–6, col. 7 ll. 31–40.

The DPC then retrieves the data in a similar fashion. J.A. 148, '988 Patent, Fig. 7; J.A. 160, '988 Patent, col. 20 ll. 11–65. It polls each DAC in its region, and, if a DAC contains additional data, it transmits that DAC to the DPC. *Id.*

After retrieving the data from the DAC, the DPC processes the data so it can be reproduced for authorized users. J.A. 149, '988 Patent, Fig. 8; J.A. 160–61, '988 Patent, col. 20 l. 66–col. 21 l. 32.

The DPC first extracts the tag header from the data, which includes sensitive information such as the customer identifier and the encryption keys to be applied to the data. J.A. 161, '988 Patent, col. 21 ll. 2–6. Using the encryption keys, the DPC decrypts the encrypted data received from the DAC. *Id.* After decompressing the data and engaging in further processing, the DPC is able to reproduce the data initially captured at a remote DAT. J.A. 149, '988 Patent, Fig. 8; J.A. 160–61, '988 Patent, col. 20 l. 66–col. 21 l. 32. This process repeats across the tiers to provide a secure, distributed remote image capturing system.

II. DataTreasury's Litigation Against the Banking Industry and Fidelity

The '988 and '137 Patents are some of the most thoroughly vetted and valuable patents in the United States. The '988 and '137 Patents are foundational to modern image-based check processing, and the vast majority of the top twenty-five banking institutions in the United States have paid hundreds of millions of dollars to license the '988 and '137 Patents.

Because of the value of the patents, many banks have fought incessantly to avoid compensating DataTreasury for use of the '988 and '137 Patents. When

DataTreasury began filing suit to protect its intellectual property, the banks instituted ex parte reexaminations against both patents in 2005. *See* U.S. Patent App. No. 90/007,830 ('137 Reexamination); and US Patent App. No. 90/007,829 ('988 Reexamination). By 2007 when the Patents were set to emerge from reexamination unchanged, the banks turned to Congress who proposed legislation that would eliminate all remedies for financial institutions' use of infringing check collection systems—such as those in the '988 and '137 Patents. Patent Reform Act of 2007, S. 1145, 110th Cong. § 14 (2007) (*available* at https://www.congress.gov/bill/110th-congress/senate-bill/1145/text#toc-id0CE1A9293A5549E1A3C61F1CAD5FC7A4, last visited on Jan. 6, 2015). That legislation failed to pass, however, after the Congressional Budget Office independently estimated that the legislation would result in a $1 billion taking. Congressional Budget Office, cost estimate for S. 1145, the Patent Reform Act of 2007 (Feb. 15, 2008), https://www.cbo.gov/sites/default/files/110th-congress-2007-2008/costestimate/s114500.pdf.

In 2010, the banks, lead by US Bank, attempted unsuccessfully to invalidate the '988 and '137 Patents through a jury trial in federal court. In that trial, US Bank raised the same arguments asserted in this instance—invalidity of the '988 and '137 Patents under 35 U.S.C. §§ 101 and 112. In fact, the defense asserted under 35 U.S.C. § 112 was the exact same argument raised in this proceeding, yet

the jury and the court soundly rejected it along with all of the other defenses. As had occurred in every instance up to this point, the resisting parties failed to invalidate the '988 and '137 Patents, and instead succeeded in reinforcing the validity and value of the patents.

Despite the herculean efforts by some entities to avoid compensating DataTreasury for the use of its intellectual property, many other banks properly obtained a license to the inventions. Large banks such as J.P. Morgan Chase Bank and PNC Bank have confessed in open court that the '988 and '137 Patents are valid. And as disclosed in open court during the trial against U.S. Bank, several banks have collectively paid in excess of $300 million to use the Patents.

DataTreasury's efforts to protect its patent rights eventually lead it to Fidelity National Information Services, Inc. While working to protect its property against infringement, DataTreasury discovered that many banks were simply relying on third-party companies, such as Fidelity, to provide the infringing check processing systems. Despite attempts by DataTreasury to license its property to Fidelity, Fidelity refused. DataTreasury had little choice but to protect its intellectual property by filing suit in 2013 against Fidelity and others. In response, Fidelity filed two petitions for CBM Review, which resulted in the present action, and three petitions for *Inter Partes* Review, all of which were denied. It is the final decisions on the two CBM Reviews that resulted in this appeal.

III. The CBM Proceedings and the PTAB Decisions

On October 25, 2013, Fidelity filed two petitions requesting post-grant review under 35 U.S.C. § 321 and § 18 of the AIA. One petition was assigned case number CBM2014-00020 and sought CBM Review of the ’137 Patent. The other petition was assigned case number CBM2014-00021, and sought CBM Review of the ’988 Patent.

A. Determinations in CBM2014-00020 Regarding the ’137 Patent

CBM2014-00020 petition made the following assertions:

- That the ’137 Patent was a covered business method patent;
- That claims 1–67 were invalid under 35 U.S.C. § 101;
- That claims 1–67 were invalid under 35 U.S.C. § 112, first paragraph because “encrypted/encrypting subsystem identification information” lacked written description; and
- That claims 1–67 were invalid under 35 U.S.C. § 112, first paragraph because transmission “within and between” the subsystems lacked written description support.

On April 29, 2014, the Board issued its decision instituting a covered business method review of the ’137 Patent. In that decision, the Board held that claims 26 and 42 were representative of the challenged claims, and construed the

terms "encrypt" or "encrypting" (claims 1, 4, 15, 26, 27, 42, and 43) and "within and between" (claims 1, 26, 42, and 43). J.A. 38–42, Institution Decision for the '137 Patent. The Board also held that the '137 Patent was eligible for CBM Review because it is directed to a financial activity, and is not a technological invention. J.A. 44–46. The Board then instituted CBM Review of claims 1–67 of the '137 Patent as "more likely than not unpatentable for lack of sufficient written description for encrypting subsystem identification information." J.A. 48. The Board also held that claims 1-67 of the '137 Patent were more likely than not "directed toward ineligible subject matter under 35 U.S.C. § 101. J.A. 52. The Board denied all of the other asserted grounds of invalidity directed toward the '137 Patent.

On April 29, 2015, the Board issued its Final Written Decision regarding the '137 Patent. In it, the Board affirmed the claim constructions from its Institution Decision and reaffirmed its institution decision that the '137 Patent was eligible for CBM Review and not a technological invention. J.A. 15–17, Final Written Decision for the '137 Patent. The Board then held that claims 1–67 of the'137 Patent were unpatentable under 35 U.S.C. § 101. J.A. 28. The Board also held that claims 1–67 lacked sufficient written description for encrypting subsystem identification information and were unpatentable. J.A. 31.

Those holdings were reaffirmed in the Board's decision on DataTreasury's request for rehearing. J.A. 1–7, Decision on Request for Rehearing for the '137 Patent.

B. Determinations in CBM2014-00021 regarding the '988 Patent

CBM2014-00021 petition made the following assertions:

- That the '988 Patent was a covered business method patent;
- That claims 1–123 were invalid under 35 U.S.C. § 101;
- That claims 1–41 and 51-69 were invalid under 35 U.S.C. § 112, first paragraph because "encrypted/encrypting subsystem identification information" lacked written description;
- That claims 1–123 were invalid under 35 U.S.C. § 112, first paragraph because transmission "within and between" the subsystems lacked written description support; and
- That claims 42–51 and 70–123 were invalid under 35 U.S.C. § 112, second paragraph because "said data processing subsystem" of claim 42 is ambiguous and "tiered architecture" and "tiered manner" of claims 42–51 and 70–123 are indefinite.

On April 29, 2014, the Board issued its decision instituting a covered business method review of the '988 Patent. In that decision the Board again held

that claims 26 and 42 were representative of the challenged claims. J.A. 120–121, Institution Decision for the '988 Patent. The Board adopted constructions for the terms "encrypt" or "encrypting" (claims 1, 4, 5, 26, 27, 120, and 123), "within and between" (claims 1, 26, 42, 46, 84, 88, 93, 97, 102, 106, 110, 114, 118, and 121), and "tiered manner/tiered architecture" (claims 42, 46, 84, 88, 93, 97, 102, 106, 110, 114, 118, and 121). J.A. 122–24, Institution Decision for the '988 Patent. The Board also held that the '988 Patent was eligible for CBM Review because it is directed to a financial activity, and is not a technological invention. *Id*. at J.A. 126–128. The Board then instituted CBM Review of claims 1–41 and 51–69 of the '988 Patent as "more likely than not unpatentable for lack of sufficient written description for encrypting subsystem identification information." J.A. 131. The Board also held that claims 1–123 of the '988 Patent were more likely than not "directed toward ineligible subject matter under 35 U.S.C. § 101." J.A. 136. The Board denied the remaining grounds of invalidity asserted against the '988 Patent.

On April 29, 2015, the Board issued its Final Written Decision regarding the '988 Patent. In it, the Board affirmed the claim constructions from its Institution Decision and reaffirmed its institution decision that the '988 Patent was eligible for CBM Review and not a technological invention. J.A. 99–100, Final Written Decision for the '988 Patent. The Board then held that claims 1–123 of the '988 Patent were unpatentable under 35 U.S.C. § 101. *Id*. at J.A. 111. The Board also

held that claims 1–41 and 51–69 lacked sufficient written description for encrypting subsystem identification information and were unpatentable. J.A. 113.

Those holdings were reaffirmed in the Board's decision on DataTreasury's request for rehearing. J.A. 84–90, Decision on Request for Rehearing for the '137 Patent.

DataTreasury timely perfected its appeal of all of the holdings of the Board.

This Court has jurisdiction under 28 U.S.C. § 1295(a)(4)(A). DataTreasury challenges the PTAB's decisions.

SUMMARY OF THE ARGUMENT

The Board's Final Written Decisions should be reversed. First, the Board lacked the power to institute CBM Review proceedings on the '988 and '137 Patents because they are patents for technological innovations. The Patents are directed to a multi-tier network computer system that utilizes remote terminals and centralized processing and storage to capture, process, encrypt, and transmit data from documents. They detail the technological components of the inventions, including computers, servers, and a technical database structure. And the legislative history of the America Invents Act indicates that these are the types of patents that Congress did not seek to extend CBM review to—computer-rooted document scanning patents whose validity has been upheld in prior administrative and judicial proceedings.

The Board's decision also suffers from problems on the merits. The Board performed a short-circuited patent-eligible subject matter analysis that improperly stripped the Patents of their computer technology-rooted claim limitations. Indeed, the Board only assessed two claims—one per patent—to invalidate nearly 200 claims. When each claim is considered individually, as *Alice* instructs, it is clear that the claims here are directed to patent-eligible subject matter: a multi-tiered network computer system that performs specific operations on specific types of data with further computer-heavy limitations.

Similarly, the Board's written description decision likewise was in error. The Board concluded that the Patents fail to describe encrypting "subsystem identification information." But the Patents expressly disclose that such information can be part of a bitmap image, which is then encrypted and transmitted. Moreover, the Patents generally disclose data encryption and a central purpose of the Patents is the secure transmission of data—which encryption of subsystem identification information furthers. Those teachings show that the Board's decisions lack substantial evidence and should be reversed. Thus, for these reasons and the reasons explained below, DataTreasury respectfully requests that the Court reverse the final decisions of the Board.

ARGUMENT

I. Standard of Review

This Court reviews the Board's factual findings for substantial evidence and reviews the Board's legal conclusions *de novo*. *In re Cuozzo Speed Techs., LLC*, 793 F.3d 1268, 1280 (Fed. Cir. 2015). With regard to the limited issue of whether the Patents are eligible for CBM review, the Board's reasoning is reviewed under the arbitrary and capricious standard while its factual determinations are subject to a substantial evidence review. *Sightsound Technologies, LLC v. Apple, Inc.*, --- F.3d ---, 2015 U.S. App. LEXIS 21640, at *14 (Fed. Cir. Dec. 15, 2015). Patent-eligibility is a question of law that this Court reviews without deference. *Versata Dev. Grp., Inc. v. SAP Am. Inc.*, 793 F.3d 1306, 1332 (Fed. Cir. 2015). The Court reviews the Board's written description decision under 35 U.S.C. § 112, ¶ 1 for substantial evidence. *In re Bimeda Research & Dev. Ltd.*, 724 F.3d 1320, 1323 (Fed. Cir. 2013).

II. The Patents Claim Technological Innovations and Thus Are Not Covered Business Methods

The Patents should not have been subjected to CBM Review, in part, because they cover technological innovations. Under Section 18 of the AIA, only certain patents are CBM-eligible: patents that claim "a method or corresponding apparatus for performing data processing or other operations used in the practice,

administration, or management of a financial product or service, except that the term does not include patents for technological inventions." Section 18(d)(1) of the AIA, 35 U.S.C. § 321; AIA § 18(d)(1), Pub. L. No. 112-29, 125 Stat. 284, 331 (2011). This definition has been carried forward into the enabling regulations adopted by the U.S. Patent & Trademark Office ("USPTO"). *See* 37 C.F.R. 42.301(a). The USPTO provided additional guidance on the meaning of this definition when it stated, "the definition of covered business method patent was drafted to encompass patents 'claiming activities that are financial in nature, incidental to a financial activity or complementary to a financial activity.'" Transitional Program for Covered Business Method Patents—Definitions of Covered Business Method Patent and Technological Invention; Final Rule, 77 Fed. Reg. 48,734, 48,735-36 (Aug. 14, 2012) (citing 157 Cong. Rec. S5432 (daily ed. Sept. 8, 2011) (statement of Sen. Schumer)). In light of the definition and explanatory clarification, neither the '988 Patent nor the '137 Patent qualify as a covered business method.

The Board committed several errors when it made the initial determination that the Patents are covered business method patents. It started by overlooking the fact that the Patents are directed to a complex data processing system that is application agnostic. J.A. 68, '137 Patent, col. 1 ll. 13–16 (explaining that the invention "relates generally to the automated processing of documents and

electronic data from different applications . . ."); J.A. 151, '988 Patent, col. 1 ll. 6–8. The agnostic nature of the invention is most telling upon review of claims of the '988 Patent—those claims do not include any reference to financial-related instruments, unlike the '137 Patent. *Compare* J.A. 161–64, '988 Patent, col. 22 l. 20–col. 28 l. 59 *with* J.A. 78–81, '137 Patent, col. 22 l. 8—col. 28 l. 45. The Board compounded its errors by stating, "We determine such activity falls within a financial product or service as it is directed to a financial activity, namely processing *financial transactions (checks)*," even though the '988 Patent never refers to checks and neither patent uses the phrase "financial transactions." J.A. 44, Institution Decision for the '137 Patent; J.A. 126, '988 Institution Decision for the '988 Patent; J.A. 55–81, '137 Patent; J.A. 139–165, '988 Patent.,

Because the specifications of both Patents include financial-related terms, however, the Board's determination that the Patents fall within the first part of the definition cannot be said to be arbitrary and capricious. *See Sightsound*, 2015 U.S. App. LEXIS 21640, at *14 (Fed. Cir. Dec. 15, 2015) (holding that the Board's reasoning is reviewed under the arbitrary and capricious standard while its factual determinations are subject to substantial evidence review). The Board repeatedly cited to statements where both patents provided a non-exclusive list of documents that can be processed by the patented inventions—"including sale, business, banking and general consumer transactions." J.A. 4, Rehearing Decision for the

'137 Patent; J.A. 44, Institution Decision for the '137 Patent; J.A. 87, Rehearing Decision for the '988 Patent; J.A. 126, Institution Decision for the '988 Patent. Listing exemplary types of paper with which the invention can be used is substantially different from limiting the invention to "activities that are financial in nature." Additionally, the use of the term "including" demonstrates the open-ended nature of the enumerated examples. *See* Manual of Patent Examining Procedure § 2111.

While a different standard of review would cause a different result, these references in the Patents are likely sufficient to prevent the initial determination that the Patents "perform[] data processing or other operations used in the practice, administration, or management of a financial product or service" from being arbitrary and capricious under the standard enumerated in *Sightsound*. 2015 U.S. App. LEXIS 21640, at *14.

The Board committed reversible error, however, when it failed to find that the Patents are technological innovations that are excluded from CBM Review. That technological nature is initially described in the abstract as "A system for remote data acquisition and centralized processing and storage . . . " J.A. 55, '137 Patent Abstract,; J.A. 139, '988 Patent Abstract. The technological nature is reinforced by the Field of the Invention, which states that "[t]his invention relates generally to the automated processing of documents and electronic data from

different applications *including* sale, business, banking and general consumer transactions." J.A. 55, '137 Patent, col. 1 ll. 13–15; J.A. 151, '988 Patent, col. 1 ll. 6–8,. The Patents continue in the Summary of the Invention stating, "The invention provides an automated, reliable, high performance, fault tolerant, and low cost system with maximal security and availability to process electronic and paper transactions, and has been named the DataTreasury™ System." J.A. 69, '137 Patent, col. 3 ll. 32–37; J.A. 152, '988 Patent, col. 3 ll. 25–29.

The Patents then detail the technological components of the invention through the figures and detailed description of how to arrange the various technical components—workstations, scanners, servers, networks, CPUs, modems, storage devices, etc.—to create the technical architecture for the different tiers of the system. *See* J.A. 69–78, '137 Patent, col. 4 l. 66–col. 22 l. 47; J.A. 152–61, '988 Patent, col. 4 l. 60–col. 22 l. 19. The Patents also detail a preferred format for capturing and storing the data and a preferred technical database structure. J.A. 77–78, '137 Patent, col. 19 l. 46–col. 22 l. 40; J.A. 155–60, '988 Patent, col. 9 l. 8–col. 19 l. 64. The Patents conclude by describing a preferred process for this complex assembly of technical components to follow when capturing the data in a preferred format, transmitting it to the various tiers, and processing and storing that data. J.A. 72–77, '137 Patent, col. 9 l. 16–col. 19 l. 45; J.A. 160–61, '988 Patent, col. 20 l. 11–col. 22 l. 12. While the inventor of the Patents did not invent each and every

component of that system, the combination of those technological components is a new and nonobvious technological innovation as demonstrated by the initial issuance of the Patents and their subsequent reexamination, from which they reissued without alteration. *See* J.A. 2027–44; J.A. 2072–84. Thus, the Board's failure to exclude the Patents from CBM Review was arbitrary, capricious, and reversible error.

That the Patents should be excluded from the definition of covered business method patent is further reinforced by the legislative history. To begin, the colloquy between Senator Pryor and Senator Leahy confirms that patents like the '988 Patent and '137 Patent should be excluded from further harassment under a CBM Review. *See* Congressional Record – Senate S5428 Sept. 8, 2011. In response to concerns raised by Senator Pryor that CBM Review could become a tool for harassing patent owners and subjecting them to substantial costs and uncertainty even after a patent had "been found valid both through previous reexaminations by the PTO and jury trials," Senator Leahy confirmed that such patents should not be subjected to a CBM review. *Id.* (Sen. Leahy stating that the heightened requirement to implement a CBM review should prevent abuse.) The Patents are exactly those types of patents—they have survived an initial examination and a reexamination by the USPTO, and they have survived a full

district court jury trial. In light of Senator Leahy's comments, the Patents should have never been subjected to CBM Review.

That same legislative history confirms that the Patents are technological inventions that are excluded from CBM Review. During consideration of the AIA, Senator Coburn specifically stated that "It is the intention of section 18 [CBM Review] to not review mechanical inventions related to the manufacture and distribution of machinery to count, sort, and *authenticate currency* like change sorters and machines *that scan paper instruments*, including currency, whose novelty turns on a technological innovation over the prior art." *Id*. The Patents do those exact things—they scan and verify paper instruments—and they do so through the technological innovation of a system that captures images and subsystem identification information, processes data, encrypts data, and transmits data across a multi-tier architecture. The novelty of that system was twice recognized by the USPTO—once during initial examination and once during reexamination—and by a jury verdict in DataTreasury's favor. Thus, the legislative history confirms that the Patents are technological innovations excluded from CBM Review, and the Board's failure to so hold was error, even under the arbitrary and capricious standard ratified in *Sightsound*.

III. The Patents Claim Patent-Eligible Subject Matter

The Board erred when it wholesale invalidated every claim of the '988 and '137 Patents for failing to claim patent-eligible subject matter. The Board improperly abstracted the disclosure and claims of the Patents to then conclude, based on one claim per Patent, that all of the claims are directed to an abstract idea. But a view of the actual claim limitations of the near-200 claims of the Patents shows that they are directed to concrete computer technology—a multi-tiered computer network architecture that processes and encrypts specific transaction data and subsystem identification information. Those same computer-heavy limitations show that, even if the Board correctly concluded that the Patents are broadly directed to transmitting encrypted information, the claim elements themselves are tied to narrow, specific applications. Lastly, the machine-or-transformation test confirms that the Patents claim patent-eligible subject matter.

A. The Abstract Idea Exception is a Narrow Exception to the Four Broad Classes of Statutory Subject Matter

Section 101 contains four broad categories of patent-eligible subject matter: "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." 35 U.S.C. § 101. It is undisputed that the Patents' claims fall within one of the four categories in § 101. The Board

concluded that the Patents fail to claim patent-eligible subject-matter under one of the exceptions to § 101: the prohibition on abstract ideas.

The abstract idea exception is narrow. First, it must be shown that the claims are directed to an abstract idea. *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2355 (2014). If so, the evidence must show that the claims—both individually and as an ordered combination—fail to transform the nature of the claim into a patent-eligible application. *Id.* The concern for preemption underpins the analysis. *Id.* at 2354, 2358. In conducting this analysis, courts "tread carefully," lest the abstract-idea exception "swallow all of patent law." *Id.* at 2354.

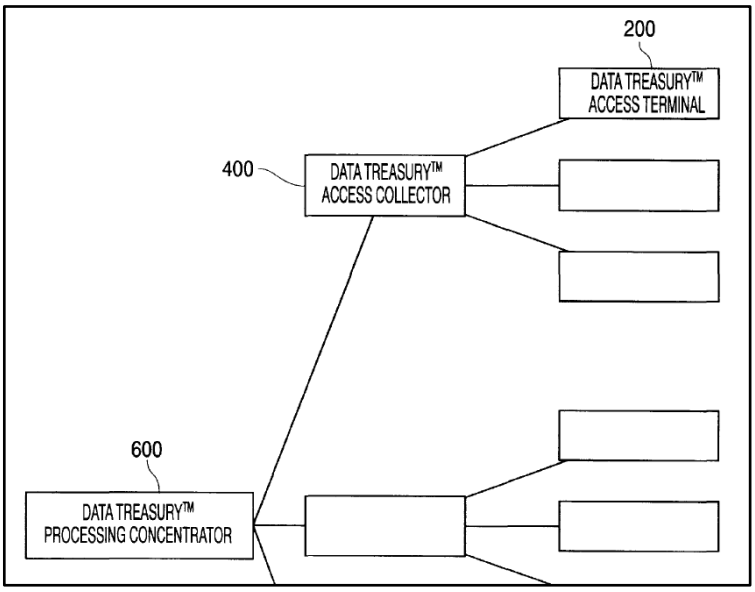
The Supreme Court has declined to "delimit the precise contours of the 'abstract ideas' category." *Alice*, 134 S. Ct. at 2356–57. However, "[w]e know that mathematical algorithms, including those executed on a generic computer, are abstract ideas" and that "some fundamental economic and conventional business practices are also abstract ideas." *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1256 (Fed. Cir. 2014) (citing *Gottschalk v. Benson*, 409 U.S. 63, 64 (1972), *Bilski v. Kappos*, 561 U.S. 593, 611 (2010), and *Alice*, 134 S. Ct. at 2356).

This Court, "in its efforts to make an 'abstract idea' less abstract," also developed the machine-or-transformation test. *Versata*, 793 F.3d at 1332. That test remains a "useful and important clue" to patent eligibility under Supreme Court precedent. *Bilski*, 561 U.S. at 604. It inquires whether the method (1) is tied

to a particular machine or (2) transforms a particular article into a different state or thing. *Id.* at 602.

B. The Claims Are Directed to Specific Networked Computer Systems, Not an Abstract Idea

The claims of the '988 and '137 Patents are directed to specific networked computer systems, not an abstract idea. The Patents are entitled "Remote Image Capture With Centralized Processing and Storage." J.A. 55, '137 Patent; J.A. 139, '988 Patent. They generally disclose a specific, tiered network computer system comprised of a series of access terminals (DATs), intermediate access collectors (DACs), and a central processing concentrator (DAC), as shown in Figure 1:



J.A. 141, '988 Patent, Fig. 1.

The DATs, DACs, and DPC are all computer systems, and the connections between them form a network structure. The Patents disclose that each DAT includes a workstation (such as a Sun Microsystem workstation), storage, a

scanner, and the like. J.A. 58, '988 Patent, Fig. 2; J.A. 153, '988 Patent, col. 5 ll. 26–39. Likewise, each DAC includes a server (such as a Windows NT-based server), storage, and similar computer components. J.A. 145, '988 Patent, Fig. 4; J.A. 156, '988 Patent, col. 11 ll. 12–49. Finally, the DPC also includes a server and workstation (such as Windows-based computers) and their associated components. J.A. 147, '988 Patent, Fig. 6; J.A. 157, '988 Patent, col. 14 ll. 19–61.

This tiered computer network architecture manifests itself in the claims of the Patents. A number of claims are directed to a specific two-tier system—a network containing a remote data access subsystem and a central data processing subsystem. *See, e.g.*, J.A. 161, '988 Patent, claim 1; J.A. 78–79, '137 Patent, claim 1. Others are directed a three-tier system—a network containing a remote subsystem, an intermediate subsystem, and a central subsystem. *See, e.g.*, J.A. 164, '988 Patent, claim 42; J.A. 79, '137 Patent, claim 18.

Within the claims, the specific tiered network architecture captures specific image data at a specifically described computer subsystem, processes the data, and then transmits the data securely through the tiered system. *See, e.g.*, J.A. 161, '988 Patent, claim 1; J.A. 78–79, '137 Patent, claim 1. Many claims also require encrypting the specific image data to securely transmit information through the tiered system—the "subsystem identification information," *i.e.*, information that identifies a specific computer within the tiered network architecture, and the

"transaction data" obtained from the document. *See, e.g.*, J.A. 161, '988 Patent, claim 1; J.A. 78–79, '137 Patent, claim 1. Moreover, dependent claims include additional computer-centric limitations, including limitations relating to the types of interfaces, software, types of bitmap images processed, and error correction. *E.g.*, J.A. 79, '137 Patent, claims 3, 4, 9, and 15; J.A. 161–62, '988 Patent, claims 3, 4, and 15.

The claims of the Patents are thus not directed to a mathematical algorithm, a fundamental economic or conventional business practice (such as hedging risk, intermediated settlement, or using advertising as currency), or the creation or management of a legal relationship (such as a transaction performance guaranty or an insurance policy). *DDR Holdings*, 773 F.3d at 1256–57, 1259 (Fed. Cir. 2014) (collecting cases). They are instead directed to specific network-tiered computer systems for capturing, processing, and transmitting specific image data that, for many claims, require the encryption of that data.

The Board only analyzed one claim from each Patent as part of its abstract idea analysis—claim 43 of the '137 Patent and claim 26 of the '988 Patent—both of which are two-tier claims. *See* J.A. 81, '137 Patent, claim 43; J.A. 163, '988 Patent, claim 26. It did not analyze ***any*** of the three-tier claims, any dependent claims, or any other independent claims. Based on its review of a single claim per Patent, the Board concluded that all of the claims of the Patents "are, in substance,

directed to the underlying idea of transferring information from one location to another where the transferred information is unreadable without a secret decoder key." J.A. 20, Final Written Decision for the '137 Patent; J.A. 103, Final Written Decision for the '988 Patent. That holding, for the reasons below, was erroneous.

1. *Alice* Required the Board to Determine Whether the Claims at Issue, Not Merely One Claim, Was Directed to an Abstract Idea

It was improper for the Board to analyze only one claim from each Patent as representative of the nearly 200 claims of the '988 and '137 Patents. *Alice* requires, under the first step of the analysis, that the Board determine if "the ***claims at issue***" are directed to an abstract idea. 134 S. Ct. at 2355 (emphasis added). But the Board did not look at each of the claims as part of its abstract idea analysis.

That was error. "[E]ach claim must be considered as defining a separate invention." *Jones v. Hardy*, 727 F.2d 1524, 1528 (Fed. Cir. 1984). While it is permissible to analyze representative claims in some cases, *e.g.*, *Content Extraction & Transmission LLC v. Wells Fargo Bank, N.A.*, 776 F.3d 1343, 1348 (Fed. Cir. 2014), the claims the Board selected from the Patents are not representative of the claims as a whole. As outlined above, some claims require a two-tier architecture; some claims a three-tier architecture; each claim requires capturing and processing specific data; some claims require encrypting that data; and some claims limit the types of interfaces, software, bitmap data, and error

correction utilized in the tiered-network system. The Board erred when it did not analyze those claim limitations, which show that the claims are directed to specific computer-based networks, not an abstract idea.

2. The Claims Are Not Broadly Drawn to Transferring Encrypted Information Between Locations

The Board also incorrectly concluded that every claim of the Patents was directed to the supposed abstract idea of "transferring information from one location to another where the transferred information is unreadable without a secret decoder key." J.A. 20, Final Written Decision for the '137 Patent; J.A. 103, Final Written Decision for the '988 Patent. The Board read out of the claims the computer-rooted limitations directed to specific two- and three-tier computer network architectures and the capturing, processing, transmitting, storing, and encrypting of specific data. It then concluded, after erasing the computer nature of the invention from the Patents, that the claims broadly covered aspects that "could be performed with pencil and paper." J.A. 21, Final Written Decision for the '137 Patent; J.A. 104, Final Written Decision for the '988 Patent. The Board's abstract idea decision was in error.

The Board's recited abstract idea is divorced from the claims and the teaching of the specification. The Board improperly cleaved from the Patents the computer nature of the invention—the capturing, processing, encrypting, and

transmitting of transaction data and subsystem identification information. Those operations necessarily require the use of computer and network technology. *See DDR Holdings*, 773 F.3d at 1257. They are not abstract ideas.

The Board also improperly erased from the invention the tiered nature of the claims and specific data that the network captures, encrypts, and transmits. Both groups of limitations illuminate that the Patents do not, as the Board reasoned, "pose a risk of unacceptable preemption" of all systems that "transfer[] information from one location to another where the transferred information is unreadable without a secret decoder key." J.A. 20, 23, ; J.A. 103, 106.

The claims are directed at specific systems with specific functionality. Some claims are directed to a two-tiered architecture and some claims are directed to a three-tiered architecture—not just any type of network.

In addition, the claims the Board deemed representative also require the tiered system to capture, encrypt, and transmit specific data—not just any type of information. Specifically, those claims delineate that the system processes, transmits, and stores transaction data captured from an image. J.A. 163, '988 Patent, claim 26; J.A. 81, '137 Patent, claim 43. They likewise recite that the system transmits subsystem identification information—*e.g.*, information that identifies a remote access computer such as the DAT—within and between the

various tiers of computers in the network. J.A. 163, '988 Patent, claim 26; J.A. 81, '137 Patent, claim 43; J.A. 2204.

Finally, the deemed representative claims require encryption of the specific transaction data and subsystem identification information by the computer—an additional technological operation. J.A. 163, '988 Patent, claim 26; J.A. 81, '137 Patent, claim 43; *TQP Development, LLC v. Intuit Inc.*, Case No. 2:12-CV-180-WCB, 2014 U.S. Dist. LEXIS 20077, at *12, *16–17 (E.D. Tex. Feb. 19, 2014) (Bryson, C.J. sitting by designation) (rejecting § 101 defense, in part, because data encryption was "a particular technological field" and, "apart from the most fanciful uses," computing devices were required to perform data encryption). Thus, the Board's recitation of an abstract idea fails when reviewing the independent claims.

The Board also erred when it did not address the additional limitations present in numerous dependent claims. Those limitations further show that the Patents are not directed to merely transferring encrypted information, but a networked computer system. *See, e.g.*, J.A. 161, '988 Patent, claim 3 (requiring the computer terminal to include a "card interface," a "signature interface," and a "biometric interface"); J.A. 161, '988 Patent, claim 4 (limiting the claims to the use of tagged bitmap-format images); J.A. 162, '988 Patent, claim 9 (requiring the claimed system to include, among other limitations, a server, a database, and specific reporting and domain name assigning software); J.A. 162, '988 Patent,

claim 15 (requiring partitioning of transaction data and providing a gateway for error correction); J.A. 2040–43, '988 Patent, claims 84, 88, 93, 97, 102, 106, and 118 (claiming a three-tiered network architecture that requires a specific network configuration and operations).

Ultimately, the Board improperly zoomed out beyond what the '988 and '137 Patents disclose and claim. As a result, the Board failed to heed *Alice*'s instruction to "tread carefully," lest the abstract-idea exception "swallow all of patent law." 134 S. Ct. at 2354. The Board thus erred when it concluded that every claim of the '988 and '137 Patents is directed towards an abstract idea.

C. The Claims Contain Sufficient Limitations to Transform Any Alleged Abstract Idea Into a Patent-Eligible Application—a Narrow, Tiered Networked Computer System That Processes, Transmits, and Encrypts Specific Data

Even assuming that the Patents are directed to an abstract idea, the claims contain sufficient elements to transform the nature of the claims into a patent-eligible application of the abstract idea. As detailed above, the claims are limited to a specific type of network architecture (a two-tier or three-tier architecture, depending on the claim), and recite the capturing, processing, transmitting, and encrypting of specific data (transaction data and subsystem identification data) within that architecture.

Thus, even under the Board's formulation of the abstract idea of "transferring information from one location to another where the transferred information is unreadable without a secret decoder key," J.A. 20–23, Final Written Decision for the '137 Patent; J.A. 103–06, Final Written Decision for the '988 Patent, the claim limitations themselves are to a specific system that encrypts and transfers specific information—they do not preempt every application of the abstract idea. Those limitations thus render the claims patent-eligible. *See DDR Holdings*, 773 F.3d at 1259 (concluding that claims directed to a "specific way to automate the creation of composite web page" did not preempt every application of "the idea of increasing sales by making two web pages look the same way").

In coming to its contrary conclusion, the Board only analyzed one claim per Patent—claim 26 of the '988 Patent and claim 43 of the '137 Patent. *See* J.A. 20, Final Written Decision for the '137 Patent; J.A. 103, Final Written Decision for the '988 Patent. It determined that the limitations in those claims failed to "limit the claim[s] in a meaningful way to avoid unacceptable preemption of the abstract idea." J.A. 17, Final Written Decision for the '137 Patent; J.A. 108–09, Final Written Decision for the '988 Patent. The Board also "reviewed the remaining challenged claims," but concluded, without analysis, that they likewise lacked sufficient limitations on the abstract idea. J.A. 19, Final Written Decision for the

'137 Patent); J.A. 110, Final Written Decision for the '988 Patent. These holdings were erroneous.

1. *Alice* Required the Board to Analyze the Elements of Each Claim—Not Merely One Claim—For an Inventive Concept

For the same reasons above with regard to the first step under *Alice*, the Board erred by analyzing only one claim from each Patent. *Alice* requires, under the second step of the analysis, the Board determine if the "***elements of each claim*** both individually and as an ordered combination" transform the nature of the claim into a patent-eligible application of an abstract idea. 134 S. Ct. at 2355 (emphases added, internal quotations omitted).

As outlined above, some claims require a two-tier architecture; some claims a three-tier architecture; each claim requires capturing and processing specific data; some claims require encrypting that data; and some claims limit the types of interfaces, software, bitmap data, and error correction utilized in the tiered-network system. For each of these claims, *Alice* required the Board to determine if those elements—both individually and as an ordered combination in the claim—were not sufficient to transform the claim into a patent-eligible application of the idea. Again, "each claim must be considered as defining a separate invention." *Jones*, 727 F.2d at 1528. And, under that analysis, the Board's eligibility decision was erroneous.

2. The Claims Contain Sufficient Limitations on the Type of Computer Network, Data, and Processing to Limit the Claims to Narrow Applications of Transferring Encrypted Data

The ’988 and ’137 Patent claims contain sufficient limitations such that the claims do not preempt all uses of an abstract idea. Even under the Board’s holding that the Patents are directed to the abstract idea of “transferring information from one location to another where the transferred information is unreadable without a secret decoder key,” J.A. 20–23, Final Written Decision for the ’137 Patent; J.A. 103–06, Final Written Decision for the ’988 Patent, the elements of each claim, individually and as an ordered combination, “do not attempt to preempt every application of the idea.” *DDR Holdings*, 773 F.3d at 1259.

As recited above, the claims delineate a specific tiered architecture of computers, scanners, modems, and related equipment, and many claims further refine the arrangement, attributes, and operations that occur within that architecture. Some of the claims require a two-tiered system, while others require a three-tiered system with separate limitations. The claims also recite the capturing, processing, transmitting, and encrypting of specific data—transaction data and subsystem identification information. Dependent claims further limit the claims to particular applications.

The Board did not address the bulk of those limitations or the combination of them in the challenged claims. Instead, relying on Dr. Alexander's declaration, the Board concluded that a three-tier architecture was "known in the art." J.A. 26, Final Written Decision for the '137 Patent; J.A. 109, Final Written Decision for the '988 Patent. But the portion of Dr. Alexander's declaration that the Board relied upon addresses the definiteness of the terms "tiered manner" and "tiered architecture" (which appear in a subset of the '983 Patent claims)—not whether the specific two-tiered and three-tiered architectures recited in the claims were conventional at the time the Patents were filed. J.A. 2139–48. And Fidelity actually submitted evidence (which the Board did not analyze) that the tiered arrangements delineated in the claims were not conventional or routine when the '988 '137 Patent was filed. *See, e.g.*, J.A. 2281–82 (expert testimony from Professor Hiles that the prior art did not render obvious the Patents)).

The Board also did not address the capturing, processing, transmitting, and encrypting of transaction data and subsystem identification information delineated in many of the claims. The Board instead concluded that DataTreasury conceded that data encryption, as a general matter, was ubiquitous. J.A. 26; J.A. 109. But the claims do not broadly cover data encryption—they are directed to encrypting specific data, namely transaction data and subsystem identification information. And the Board did not address the unconventional nature of capturing,

transmitting, processing, and encrypting subsystem identification data along with the transaction data. That is, the claims recite a linking of the captured transaction data with subsystem identification information to help track particular transaction data as it flows through the tiered architecture. There is no evidence relied upon by the Board to show those aspects of the claim were merely conventional.

Nor does the Board address whether the combination of a tiered system along with those specific data processing attributes would have been conventional. That is equally true for the dependent claims. Under *Alice*, the focus is on ***both*** individual claim elements ***and*** the combination of those elements for each challenged claim. 134 S. Ct. at 2355. But the Board only addressed two specific aspects individually—the three-tier architecture and data encryption generally (which is not a claim element; the claims require encryption of specific information). The Board did not address, as required by *Alice*, how the combination of elements affected the patent-eligibility of the claims. And, as discussed above, the claims include "additional features" that ensure that the claims are not a drafting effort to monopolize the abstract idea of transferring encrypted information. *DDR Holdings*, 773 F.3d at 1259. The Board erred when it reached a contrary conclusion.

D. The Claims Are Tied to a Specific-Tiered Network System and Transform the State of that System

The Board also erred in its application of the machine-or-transformation test, which is a "useful and important clue" to patent-eligibility and confirms that the Patents claim patent-eligible subject matter. *Bilski*, 130 S. Ct. at 3224, 3227. The Board concluded that, because the claims "involve the use of generic, well-known machines," they fail the machine-or-transformation test. J.A. 27, Final Written Decision for the '137 Patent; J.A. 110, Final Written Decision for the '988 Patent. As explained above, however, the claims are tied to specific machines—a multi-tiered architecture that performs specific operations on specific types of data—and the processing, encrypting, and transmitting operations transform the data and those machines into a different state. Although some of the components of those architectures may be considered "conventional" building blocks, the novel and particular arrangement of those components in those two-tier and three-tier architectures creates a specific machine whose operations transform that machine and the specific data it operates on. Thus, the Board erred when it concluded that all of the claims of the Patents fail the machine-or-transformation test.

* * * * *

The '988 and '137 Patents claim patent-eligible subject matter. Accordingly, DataTreasury respectfully requests that this Court reverse the

Board's finding that all of the claims of the '988 and '137 Patents fail to claim patent-eligible subject matter.

IV. The Patents Adequately Describe the "Encrypting Subsystem Identification Information" Limitation

The Patents adequately describe the "encrypting subsystem identification information" limitation. Fidelity bore the burden before the Board to show that the Patents failed to "describe an invention understandable to that skilled artisan and show that the inventor actually invented the invention claimed." *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 589 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc); 35 U.S.C. § 326(e); AIA § 18(a)(1). Fidelity did not meet that burden, and the Board's contrary conclusion lacks substantial evidence. The disputed limitation relates to encrypting computer data, and the common written descriptions of the Patents broadly disclose the encryption of information, including information listed on the face of a receipt. Moreover, the Patents expressly disclose that exemplary "subsystem identification information" may be listed on the face of the receipt and thus encrypted. Lastly, a central purpose of the Patents—the secure communication of computer information—further shows that the inventor possessed the encryption of subsystem identification information. The Board thus erred when it found that the "encrypting subsystem identification information" limitation lacked adequate written description.

A. The Patents Broadly Disclose Encryption of Computer Data, and "Subsystem Identification Information" is Computer Data

It is undisputed that the Patents teach the encryption of computer information transmitted from the DAT computer system. For example, embodiments of the Patents expressly disclose the encryption of various types of transaction data, identification data, bitmap images, and data represented by a DataGlyph™ image. *E.g.*, J.A. 151, 153–54, '988 Patent, col. 1 ll. 9–14, col. 5 l. 66–col. 7 l. 6, col. 7 ll. 31–40.

Regardless of how the computer information is labeled, computer data is a series of digital bits—logically embodied in 0s and 1s. *See* J.A. 153, '988 Patent, col. 5 l. 66–col. 6 l. 6 (explaining that each aspect of a DataGlyph™ "represent a binary 0 or 1"). Computer encryption processes operate at that digital level and are agnostic to what label is placed on the data. *See* J.A. 153, '988 Patent, col. 6 ll. 3–6 (teaching that "encryption methods, as known to persons of ordinary skill in the art encrypt the data represented by the DataGlyph™ Technology"); *see also* J.A. 2130–31 (disclosing encryption schemes that encrypt computer data without regard to what the data is labeled). Indeed, the Patents teach that a computer workstation—the DAT controller—performs encryption. J.A. 142, '988 Patent, Fig. 2; J.A. 154, '988 Patent, col. 7 ll. 31–40.

Thus, one of ordinary skill in the art would conclude that the Patents broadly disclose the encryption of transmitted data, regardless of its label. That is reinforced by how the Patents describe the invention at a more general level: "The invention provides . . . [a] system with maximal security." J.A. 152, '988 Patent, col. 3 ll. 26–29. Failing to encrypt transmitted data could jeopardize that security.

The "subsystem identification information" is one type of digital data, again represented by a string of 0s and 1s. There is nothing special or unique about the data that precludes it from being encrypted by the DAT controller. To the contrary, as discussed below, the Patent teaches that it may be encrypted as part of the encrypted bitmap image.

The Board did not address the Patents' broader disclosure of data encryption. Nor did Dr. Alexander's declaration, the sole evidence upon which the Board relies, J.A. 6–7, Rehearing Decision for the '137 Patent; J.A. 89–90, Rehearing Decision for the '988 Patent. Instead, the Board reasoned that the "encrypting subsystem identification information" limitation lacked written support because the Board found that the Patents do "not describe encrypting *all* of the transferred information." J.A. 6, Rehearing Decision for the '137 Patent (emphasis added); J.A. 89, Rehearing Decision for the '988 Patent (emphasis added). It thus concluded that DataTreasury "failed to demonstrate that [it]

possessed the invention." J.A. 7, Rehearing Decision for the '137 Patent; J.A. 90, Rehearing Decision for the '988 Patent.

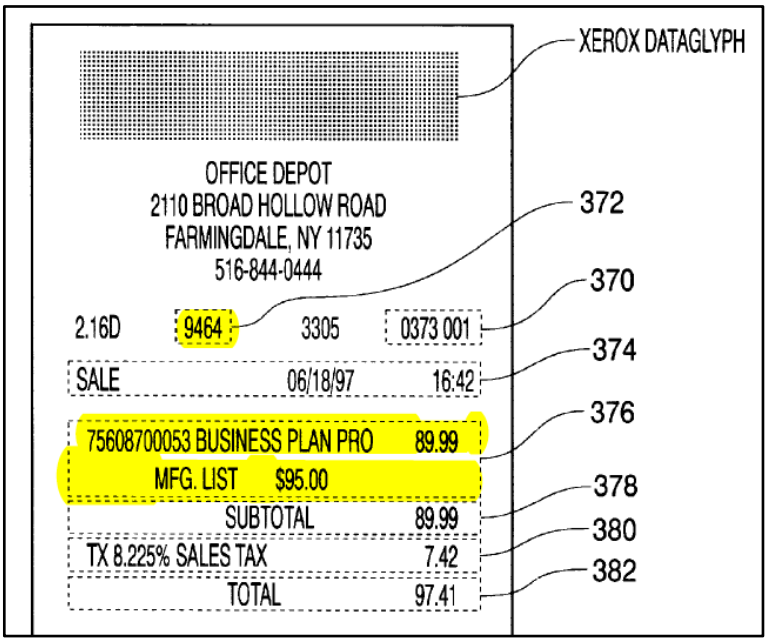
That was error. The Board applied an overly stringent written description standard and flipped the burden of proof. The Patents need not expressly disclose encryption of ***all*** of the transferred information to have written description support. And it was not DataTreasury's burden to prove written description. 35 U.S.C. § 326(e); AIA § 18(a)(1). Instead, Fidelity needed to show that the Patents lacked sufficient disclosure of encrypted data such that skilled artisans would conclude that the inventor did not possess encrypting data labeled "subsystem identification information." *See Ariad*, 598 F.3d at 1352.

The disclosure in the Patents, however, shows that the Board's decision must be reversed under the correct standard. The Patents teach that data of any label can be encrypted, they do not exclude subsystem identification information as encryption-worthy data, and they specifically describe the invention as providing security. Moreover, as detailed below, the Patents expressly disclose that subsystem identification information can be included within a bitmap image that the system encrypts. That disclosure further shows that the Board's decision lacks substantial evidence.

B. The Patents Expressly Disclose Encrypting Bitmap Image Data, Which May Include "Subsystem Identification Information"

The Patents contain a specific disclosure of encrypted "subsystem identification information." The Board failed to meaningfully address that teaching, and the disclosure demonstrates that the Board's ultimate written description finding lacks substantial evidence.

It is undisputed that the Patents disclose that the system encrypts bitmap image data. *E.g.*, J.A. 154, '988 Patent, col. 7 ll. 31–40. Those bitmap images can include two sets of data: (1) transaction data, such as the price or item name, labeled 376 below; and (2) identification information, such as the credit card terminal identifier, labeled 372 below. J.A. 144, '988 Patent, Fig. 3B; J.A. 155, '988 Patent, col. 9 l. 33–col. 10 l. 26, col. 10 ll. 61–67.



J.A. 144, '988 Patent, Fig. 3B (truncated and highlighting added)

In addition to the exemplary data depicted in the image, the Patents also teach that the identification information on the bitmap image may include "the DAT 200," *i.e.*, information that identifies the DAT used by the customer (which is an exemplary remote subsystem):

> As is known to persons of ordinary skill in the art, the DataTreasury™. System 100 can also process receipts with alternate formats as long as ***the receipt contains the appropriate identification information such as . . . the DAT 200 . . . etc.***

J.A. 155, '988 Patent, col. 10 ll. 61–67 (emphasis added). Thus, the Patents teach that the identification information of the DAT may be encrypted.

The Board failed to meaningfully address this teaching. Dr. Alexander's declaration, upon which the Board relied, likewise does not address the disclosure of the "DAT 200" as information included as part of exemplary bitmap image data. *See* J.A. 2123–34. The Board instead found that the Patents' disclosure was insufficient because "[t]he claims require encrypting 'subsystem identification information,' and not merely 'identification information.'" J.A. 22, Final Written Decision for the '137 Patent; J.A. 112, Final Written Decision for the '988 Patent. That was error.

The disclosure of encrypted "identification information," along with the disclosure of other encrypted data, shows that those of skill in the art would conclude that the inventor possessed encrypting "subsystem identification

information." Encryption of each type of data occurs at the digital level, irrespective of the label. But instead of considering that evidence, the Board erred when it applied the law. It searched for the exact words "subsystem identification information" without considering the Patents' entire teaching. *Ariad*, 589 F.3d at 1351 (holding that the written description inquiry looks to "the four corners of the specification" and explaining that the specification does not need to recite "the claimed invention in *haec verba*" to provide adequate written description).

In that overly narrow search, the Board overlooked the express teaching that DAT identification information—undisputedly one type of "subsystem identification information, *see* J.A. 2204 (construing "subsystem identification information")—can be part of an encrypted bitmap image and thus encrypted. That express disclosure conclusively demonstrates that the inventor had possession of the claimed invention. And it shows that the Board's decision cannot be upheld.

C. The Board's Focus on Encryption of Tag Headers Was in Error

The Board also found a lack of written description support because the Patents do not "describe any encryption to the tag headers." J.A. 22, Final Written Decision for the '137 Patent; J.A. 113, Final Written Decision for the '988 Patent. The claims, however, are not limited to "tag headers," but "subsystem identification information," which may or may not be embodied in a header. And,

as recited above, there is ample support in the specification that conclusively shows that the inventor possessed encryption of subsystem identification information.

In any event, the Patents also demonstrate that, contrary to the Board's finding, the inventor possessed the encryption of the tag headers, even though the encryption of that data is not disclosed in *haec verba* in the Patents. A central purpose of the Patents is to provide for secure and encrypted communication of information from the DAT to a central processing source. *See, e.g.*, J.A. 139, '988 Patent, Abstract. To that end, the Patents disclose encryption of information that is transmitted from the DAT. *See, e.g.*, J.A. 153–54, '988 Patent, col. 5 l. 46–col. 6 l. 7, col. 7 ll. 31–40, col. 8 ll. 3–5. Prior to the transmission, a tag is prepended to the transaction data. That tag includes, among other information, the encryption keys that, upon receipt, are used to decrypt the data. J.A. 160–61, '988 Patent, col. 20 l. 66–col. 21 l. 6. The DAT then transmits the combined information to the centralized system. Thus, if those encryption keys were always transmitted in the "clear," *i.e.*, without encryption—as the Board found—the system would not be secure because any party receiving the transmission would also receive the encryption keys and could then use those keys to decrypt the transaction data.

As DataTreasury's technical expert explained—and the Board failed to address—such an unsecure system would be equivalent to locking a secure box

and then stamping the lock's combination on the back of the lock. *See* J.A. 2283–84; J.A. 2295–96. That implementation would defeat a central purpose of the Patent—the secure communication of sensitive information. The Patents' emphasis on security forecloses the Board's overly narrow reading of the specification as only disclosing the transmission of non-encrypted tags. Indeed, the Board even recognized in another part of the Decision that the Patent was directed to using a "secret decoder key." J.A. 20, Final Written Decision for the '137 Patent; J.A. 103, Final Written Decision for the '988 Patent.

* * * * *

The '988 and '137 Patents adequately describe the "encrypting subsystem identification information" limitation. Accordingly, DataTreasury respectfully requests that this Court reverse the Board's finding that claims 1–67 of the '137 Patent and claims 1–41 and 51–69 of the '988 Patent lack written description support.

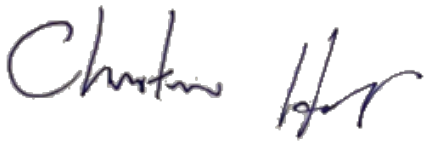
CONCLUSION AND STATEMENT OF RELIEF SOUGHT

The Board erred when it concluded that the '988 and '137 Patents were CBM-eligible. After committing that jurisdictional error, it then erred on the merits, holding that the Patents fail to claim patent-eligible subject matter and are not adequately described. The Patents, however, are directed to computer network technology and adequately describe the use of encryption as part of that

technology. Thus, DataTreasury respectfully requests that this Court reverse the Final Written Decisions of the Board.

Dated: January 6, 2016

Respectfully submitted,



CHRISTIAN HURT

DEREK GILLILAND
NIX PATTERSON & ROACH, L.L.P.
205 Linda Drive
Daingerfield, Texas 75638
903.645.7333 (telephone)
903.645.5389 (facsimile)
dgilliland@nixlawfirm.com

EDWARD CHIN
CHRISTIAN HURT
NIX PATTERSON & ROACH, L.L.P.
5215 N. O'Connor Blvd., Suite 1900
Irving, Texas 75039
972.831.1188 (telephone)
972.444.0716 (facsimile)
edchin@me.com
christianhurt@nixlawfirm.com

Attorneys for Appellant
DataTreasury Corporation

ADDENDUM

ADDENDUM

Trials@uspto.gov
571-272-7822

Paper 42
Entered: July 30, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FIDELITY NATIONAL INFORMATION SERVICES, INC.,
Petitioner,

v.

DATATREASURY CORP.,
Patent Owner.

Case CBM2014-00020
Patent 6,032,137

Before MICHAEL P. TIERNEY, WILLIAM V. SAINDON, and MATTHEW R. CLEMENTS, *Administrative Patent Judges*.

TIERNEY, *Administrative Patent Judge*.

DECISION
DataTreasury's Request for Rehearing
of Final Written Decision
37 C.F.R. § 42.71

I. STATEMENT OF THE CASE

On April 29, 2015, we entered a Final Written Decision in which we found claims 1–67 of U.S. Patent No. 6,032,137 ("the '137 Patent") to be unpatentable. Paper 34 ("Final Dec."). Patent Owner, DataTreasury Corp., has filed a request for rehearing of that decision. Paper 41 ("Req. Reh'g."). For the reasons discussed below, Patent Owner's Request for Rehearing is denied.

II. THE REQUEST FOR REHEARING

Patent Owner seeks reconsideration based on the following main contentions: (a) the Board erred in determining that the '137 patent is a covered business method patent; (b) the Board erred in determining that the challenged claims are directed to patent ineligible subject matter; and (c) the Board erred in determining that the challenged claims lacked sufficient written description for encrypting the claimed subsystem identification information.

We have reviewed Patent Owner's request for rehearing and carefully considered Patent Owner's arguments. Our decision on rehearing addresses the main arguments presented by Patent Owner. We have, however, considered all of the arguments presented, including those not addressed specifically in this decision. We are not persuaded that the Board misapprehended or overlooked Patent Owner's arguments presented in its response or evidence with respect to the patentability of the challenged claims.

III. ANALYSIS

In pertinent part, 37 C.F.R. § 42.71(d) states:

> The burden of showing a decision should be modified lies with the party challenging the decision. The request must specifically identify all matters the party believes the Board misapprehended or overlooked, and the place where each matter was previously addressed in a motion, an opposition, or a reply.

Patent Owner's main arguments presented in its request for rehearing are addressed below.

A. The '137 patent is a Covered Business Method Patent

Patent Owner contends that the '137 patent is not eligible for covered business method review as the '137 patent is directed to "a specific data processing system that is application agnostic." Req. Reh'g. 2. Additionally, Patent Owner contends that the Board erred in holding that the '137 patent does not claim a technological invention. *Id*. at 4. We have considered Patent Owner's arguments but are not persuaded that we misapprehended or overlooked that the subject matter of the '137 patent is eligible for covered business method review.

Our Decision to Institute (Paper 13) held that the '137 patent is directed to financial activity, processing financial transactions, and constitutes a financial service or product. Dec. to Inst. 10–11. Patent Owner's contention that the '137 patent is application agnostic fails to address our prior finding that the patent states that it is directed to financial products and services by capturing an image of financial transaction data. *Id*.

Patent Owner cites the ’137 specification’s “Field of Invention” at column 1, lines 9–14 for the proposition that the data is not limited to a particular application. Req. Reh’g 2. Patent Owner however, overlooks the fact that the Field of the Invention section begins by stating:

> This invention relates generally to the automated processing of documents and electronic data from different applications including sale, business, banking and general consumer transactions.

Ex. 1001, 1:5–9. As apparent from the ’137 patent, the claimed data processing system is directed to a financial service or product.

Patent Owner also contends that the Board erred in holding that the ’137 patent does not claim a technological invention. Req. Reh’g. 4. According to Patent Owner, “[t]he [’137] Patent is directed to a new and distinct arrangement of computer components that transmit data in a new way.” *Id*. Patent Owner however, does not show where the Board erred in its Decision to Institute, which held that none of the steps of representative claim 26 recites a novel and unobvious technological feature. Dec. to Inst. 12–13. This holding was reaffirmed in the Final Written Decision. Final Dec. 8–9.

B. The Challenged Claims are Directed to Patent Ineligible Subject Matter

Patent Owner states that the Board erred in concluding that the ’137 patent fails to claim patent-eligible subject matter. Req. Reh’g. 4. According to Patent Owner, the Board improperly considered only one claim—claim 43—as representative, and failed to consider each of the 67 claims in the patent. *Id*. at 5–6. For example, Patent Owner contends that

the Board did not address additional limitations, such as the card interface of claim 3, the tagged bitmap format images of claim 4, and the domain name assigning software of claim 9. *Id*. at 8. Additionally, Patent Owner also disputes the Board's determination that the claims are directed to an abstract idea, the determination that the claims improperly preempt the abstract idea, and the Board's failure to discuss both precedent and the '137 patent's tiered networked teachings. *Id*. at 4–11.

We have considered Patent Owner's contentions but do not find them persuasive. For example, although Patent Owner contends that the Board did not address certain limitations in its 67 challenged claims, Patent Owner does not identify where these particular limitations were discussed in its Patent Owner Response. Arguments not raised in the briefs before the Board and evidence not previously relied upon in the briefs are not permitted in the request for rehearing. Additionally, as stated in the Final Written Decision, the Board considered each of the challenged claims and was persuaded based on the evidence presented that the claims lacked limitations that meaningfully limited the abstract idea. Final Dec. 17–20. In particular, the Board credited the testimony of Petitioner's expert, Dr. Alexander, that the '137 patent claims merely arrange old, well-known elements with each performing the same function it had been known to perform. *Id*. Dr. Alexander's testimony addresses each of the now-disputed limitations, e.g., card interface (claim 3), tagged bitmap format images (claim 4), and domain name assigning software (claim 9) and demonstrates that the limitations merely recite a known set of prior art elements used according to their established functions. Ex. 1003 ¶¶ 104–138.

C. The Challenged Claims Lacked Sufficient Written Description

Patent Owner contends that Petitioner failed to prove that the '137 patent claims lack written description for "'encrypting subsystem identification information'" limitation in claims 1–67. Req. Reh'g. 11–15. According to the Patent Owner, the Board erroneously placed the burden of proof on the Patent Owner to demonstrate written description and disregarded the disclosure of the '137 patent that its system is capable of encrypting all of the transferred information. *Id*. Patent Owner cites the following phrase from the Final Written Decision: "'to demonstrate that Patent Owner possessed the invention'" as evidence that the Board placed the burden on the Patent Owner to prove written description. *Id*. at 12. To place the phrase in context, the Final Written Decision states:

> The claims require encrypting "subsystem identification information" and not merely "identification information." Patent Owner's citations to the '137 patent specification fail to demonstrate that Patent Owner possessed the invention. As recognized by Dr. Alexander, one skilled in the art would understand that the '137 patent specification does not describe any encryption to the tag headers that are prepended to the ECBI. Ex. 1003 ¶¶ 149–159.

Final Dec. 22. As apparent from the Final Written Decision, the burden of proof was placed on Petitioner. The Board credited the testimony of Petitioner's expert, Dr. Alexander, and held that Petitioner met its burden and demonstrated that the '137 patent does not describe encrypting all of the transferred information. Specifically, the Final Written Decision states:

> Based on the evidence of record, we credit the testimony of Dr. Alexander and agree with Petitioner that:

> (1) the specification fails to describe encrypting the DAT_TERMINAL_ID;
> (2) generic "identification information" does not constitute the claimed subsystem identification information; and
> (3) subsystem identification information is not included in the "paper transaction data" of the disclosed receipt.
>
> Reply 12–13. We find that Petitioner has demonstrated that claims 1–67 are unpatentable for lack of sufficient written description for encrypting subsystem identification information.

Final Dec. 22–23.

In consideration of the above, the Patent Owner's Request for Rehearing is DENIED.

CBM 2014-00020
Patent 6,032,137

For PETITIONER:

Erika H. Arner
Darren M. Jiron
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.
erika.arner@finnegan.com
darren.jiron@finnegan.com
FIS-Ballard@finnegan.com

For PATENT OWNER:

Abraham Hershkovitz
Eugene C. Rzucidlo
HERSHKOVITZ & ASSOCIATES, PLLC
AHershkovitz@Hershkovitz.net
GRzucidlo@Hershkovitz.net

Trials@uspto.gov
571-272-7822

Paper 34
Entered: April 29, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FIDELITY NATIONAL INFORMATION SERVICES, INC.,
Petitioner,

v.

DATATREASURY CORP.,
Patent Owner.

Case CBM2014-00020
Patent 6,032,137

Before MICHAEL P. TIERNEY, WILLIAM V. SAINDON, and MATTHEW R. CLEMENTS, *Administrative Patent Judges*.

TIERNEY, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
Covered Business Method Patent Review
35 U.S.C. §328(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

Fidelity National Information Services, Inc. ("Fidelity" or "Petitioner") filed a Petition ("Pet.") requesting review under the transitional program for covered business method patent review of claims 1–67 of U.S. Patent No. 6,032,137 ("the '137 patent") (Ex. 1002). On April 29, 2014, pursuant to 35 U.S.C. § 324, we instituted this trial as to claims 1–67 on two ground of unpatentability under 35 U.S.C. §§ 101 and 112, first paragraph, lack of written description (Paper 13, "Dec. on Inst."). Patent Owner DataTreasury Corp. ("Patent Owner" or "DataTreasury") filed a Patent Owner Response (Paper 24, "PO Resp."), and Petitioner filed a Reply (Paper 25, "Reply").

Patent Owner filed a Motion to Exclude Petitioner's demonstratives. Paper 30. Patent Owner subsequently withdrew its Motion to Exclude. Paper 32.

An oral hearing in this proceeding was held on December 9, 2014. A transcript of the hearing is included in the record (Paper 33, "Tr.").

We have jurisdiction under 35 U.S.C. § 6(c). This Final Written Decision is issued pursuant to 35 U.S.C. § 328(a) and 37 C.F.R. § 42.73.

For the reasons that follow, we determine that Fidelity has shown by a preponderance of the evidence that claims 1–67 of the '137 patent are unpatentable under 35 U.S.C. § 101 and unpatentable under 35 U.S.C. § 112, first paragraph, for lack of written description.

A. The '137 Patent (Ex. 1002)

The '137 patent is directed to a system for remote data acquisition, and centralized processing and storage of the acquired data. Ex. 1002,

Abstract. An object of the invention is to provide an automated system to manage and store captured electronic and paper transactions from various activities including banking and consumer applications. *Id.* at 3:22–26. Generally, the '137 patent describes scanning documents using a scanner attached to a general purpose network computer that is connected via a carrier cloud to a server that inserts images and data received into a database. *Id*. at Figs. 1–2, 3:37–58, 4:65–5:15, 5:45–51, 16:53–60. Additionally, the general purpose network computer encrypts the images and data to provide a system with maximal security. *Id*. at 3:30–36, 7:38–46, 8:10–15.

Figure 1 of the '137 patent, provided below, depicts a preferred embodiment of the system having three major operational elements:

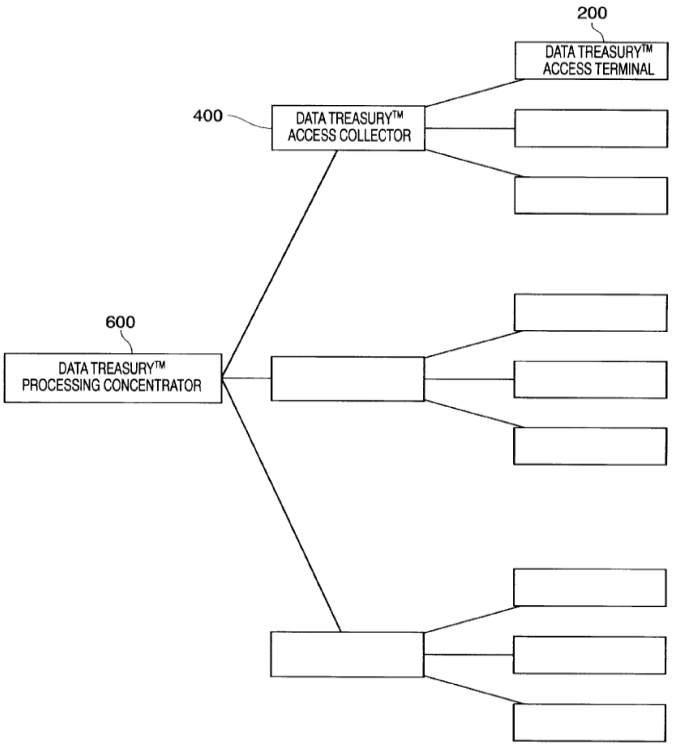


FIG. 1

The '137 patent describes the tiered arrangement depicted in Figure 1 as follows:

> FIG. 1 shows the architecture of the DataTreasury™ System 100. The DataTreasury™ System 100 has three operational elements: the DataTreasury™ System Access Terminal (DAT) 200 (the remote data access subsystem), the DataTreasury™ System Access Collector (DAC) 400 (the intermediate data collecting subsystem), and the DataTreasury™ System Processing Concentrator (DPC) 600 (the central data processing subsystem).

Id. at 4:66–5:6.

Figure 2 of the ’137 patent, provided below, depicts a block diagram of the DAT (remote data access subsystem terminal):

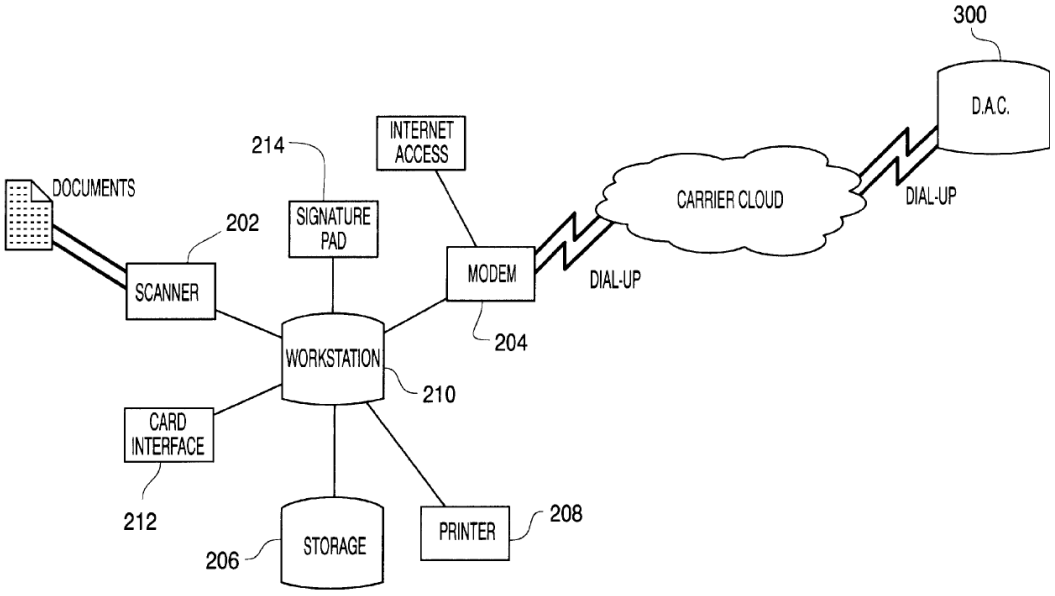


FIG. 2

As shown in Figure 2, scanner 202 is connected to workstation 210, which is connected to data system access collector 300. The workstation can be a general purpose computer and performs tasks including compressing, encrypting, and tagging a scanned bitmapped image. *Id*. at 5:40–45, 7:31–35.

The ’137 patent is said to improve upon the prior art by providing an automated, reliable, secure system to process electronic and paper transactions. *Id*. at 3:32–37.

B. Illustrative Claims

Of the challenged claims, claims 1, 26, 42, and 43 are independent claims. Independent claims 26 and 43 are illustrative of the challenged claims in the ’137 patent and are reproduced below:

> 26. A method for central management, storage and verification of remotely captured paper transactions from checks comprising the steps of:
>
> capturing an image of the paper transaction data at one or more remote locations including a payer bank’s identification number, a payer bank’s routing number, a payer bank’s routing information, a payer’s account number, a payer’s check, a payer bank’s draft, a check amount, a payee bank’s identification information, a payee bank’s routing information, and a payee’s account number; and sending a captured images of the transaction data;
>
> managing the capturing and sending of the transaction data;
>
> collecting, processing, sending and storing the transaction data at a central location;
>
> managing the collecting, processing, sending and storing of the transaction data;
>
> encrypting subsystem identification information and the transaction data; and
>
> transmitting the transaction data and the subsystem identification information within and between the remote location(s) and the central location.

> 43. A method for central management, storage and verification of remotely captured paper transactions from checks comprising the steps of:

capturing an image of the check at one or more remote locations and sending a captured image of the check;

managing the capturing and sending of the transaction data;

collecting, processing, sending and storing the transaction data at a central location;

managing the collecting, processing, sending and storing of the transaction data;

encrypting subsystem identification information and the transaction data;

verifying the transaction data from the check; and

transmitting the transaction data and the subsystem identification information within and between the remote location(s) and the central location.

C. Related Proceedings

Petitioner indicates that the '137 patent is asserted in *DataTreasury Corp. v. Fidelity National Information Services, Inc*., No. 2:13-cv-432 (E.D. Tex.) in the U.S. District Court for the Eastern District of Texas ("the District Court"). Pet. 16. Petitioner also identifies an additional twenty-three district court proceedings involving the '137 patent. Pet. 4–6.

D. Alleged Grounds of Unpatentability Instituted in Trial

Petitioner contends that the challenged claims are unpatentable based on the following grounds:

Grounds	Claims Challenged
§ 101	1–67
§ 112, 1st ¶, Written Description	1–67

II. ANALYSIS

A. Claim Construction

The Board interprets claims of unexpired patents using the "broadest reasonable construction in light of the specification of the patent in which [they] appear[]." 37 C.F.R. § 42.300(b); *see* Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,766 (Aug. 14, 2012) ("Trial Practice Guide"); *In re Cuozzo Speed Techs., LLC*, 778 F.3d 1271, 1281 (Fed. Cir. 2015); *In re Translogic Tech., Inc*., 504 F.3d 1249, 1257 (Fed. Cir. 2007); *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). Claim terms are given their plain and ordinary meaning as would be understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. "There are only two exceptions to this general rule: 1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution." *Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

In the Decision on Institution, we interpreted various claim terms of the '137 patent as follows:

Claim Term (Claims)	Interpretation
"encrypt" or "encrypting" (1, 4, 5, 26, 27, 42, and 43)	Convert into a form unreadable by anyone without a secret decryption key.
"within and between" (1, 26, 42, and 43)	Data is transmitted both within a given subsystem (i.e., between the various components comprising the subsystem or location) and between one subsystem or location to another subsystem or location.

See Dec. on Inst. 7–9. The parties do not dispute these interpretations in their Patent Owner Response and Reply. We adopt the above claim constructions based on our previous analysis, and see no reason to deviate from those constructions for purposes of this decision.

B. Covered Business Method Patent

We determined, in the Decision on Institution, that the '137 patent is a covered business method patent as defined in § 18(a)(1)(E) of the America Invents Act and 37 C.F.R. § 42.301, because at least one claim of the '137 patent is directed to a covered business method. Dec. on Inst., 9–13.

The definition of "covered business method patent" in Section 18(d)(1) of the AIA excludes patents for "technological inventions." Patent Owner contends that the Board erred in instituting this proceeding alleging that every claim of the '137 patent recites a technological invention. PO Resp. 10–14.

Patent Owner states that every system claim and every subsystem claim in the '137 patent is directed to technological equipment and provides a solution to the transmission of financial information. *Id*. at 10. Patent Owner further contends that every method claim recites steps performed by technological equipment. *Id*. at 10–11. The challenged claims, however, merely require the use of "off the shelf" technology, including conventional

imaging scanners attached to a general purpose computer network. *Id*. at 13; Ex. 1003 (Declaration of Dr. Peter Alexander)[1] ¶¶ 105–111.

Patent Owner states that its system is a technological invention because its claims are directed to a three-tiered system including three subsystems and therefore, is a technological banking system that is new, useful and nonobvious. PO Resp. 12–13. Patent Owner fails to explain how a three-tier system is a technological invention. For example, the three-tier system can be viewed as reflecting a banking system having networked branch offices, regional offices and a central home office.

We have considered Patent Owner's remaining arguments and evidence regarding its contention that all the claims of the '137 patent are directed to a technological invention, but are not persuaded that its system and method claims recite a technological feature that is novel and unobvious over the prior art. We reaffirm our determination in the Decision on Institution and conclude that the '137 patent is eligible for a covered business method patent review.

C. Grounds Based on 35 U.S.C. § 101— Claims 1–67 Are Directed to Non-Statutory Subject Matter

Petitioner challenges claims 1–67 of the '137 patent under 35 U.S.C. § 101, as directed to patent-ineligible subject matter. Pet. 20–37. Patent Owner disagrees and maintains that its claims are directed to patent-eligible processes because the claims do not recite an abstract idea. PO Resp. 28–66. For example, Patent Owner states:

---

[1] We conclude that Dr. Alexander is qualified to testify as to the understanding of one skill in the art in this proceeding. *See* Ex. 1003 ¶¶ 1–4.

> With respect to §101, the real issue in this CBM Proceeding is whether the teaching of scanning or imaging of documents and receipts is an "abstract idea."

Id. at 46.

1. Section 101 Subject Matter Eligibility

For claimed subject matter to be patent eligible, it must fall into one of four statutory classes set forth in 35 U.S.C. § 101: a process, a machine, a manufacture, or a composition of matter. The Supreme Court recognizes three categories of subject matter that are ineligible for patent protection: "laws of nature, physical phenomena, and abstract ideas." *Bilski v. Kappos*, 561 U.S. 593, 601 (2010) (internal quotations and citation omitted). A law of nature or an abstract idea by itself is not patentable; however, a practical application of the law of nature or abstract idea may be deserving of patent protection. *Mayo Collaborative Servs. v. Prometheus Labs., Inc*., 132 S. Ct. 1289, 1293–94 (2012). To be patentable, however, a claim must do more than simply state the law of nature or abstract idea and add the words "apply it." *Id*.

In *Alice Corp. Pty, Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014), the Supreme Court recently clarified the process for analyzing claims to determine whether claims are directed to patent-ineligible subject matter. In *Alice*, the Supreme Court applied the framework set forth previously in *Mayo*, "for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of these concepts." *Alice*, 134 S. Ct. at 2355. The first step in the analysis is to "determine whether the claims at issue are directed to one of those patent-ineligible concepts." *Id*. If they are directed to a patent-

ineligible concept, the second step in the analysis is to consider the elements of the claims "individually and 'as an ordered combination'" to determine whether there are additional elements that "'transform the nature of the claim' into a patent-eligible application." *Id*. (quoting *Mayo*, 132 S. Ct. at 1291, 1297). In other words, the second step is to "search for an 'inventive concept'—i.e., an element or combination of elements that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'" *Id*. (alteration in original) (quoting *Mayo*, 132 S. Ct. at 1294). Further, the "prohibition against patenting abstract ideas 'cannot be circumvented by attempting to limit the use of the formula to a particular technological environment' or adding 'insignificant postsolution activity.'" *Bilski*, 561 U.S. at 610–11 (quoting *Diamond v. Diehr*, 450 U.S. 175, 191–92 (1981)).

The patents at issue in *Alice* claimed "a method of exchanging financial obligations between two parties using a third-party intermediary to mitigate settlement risk." *Alice*, 134 S. Ct. at 2356. Like the method of hedging risk in *Bilski v. Kappos*, 561 U.S. at 628—which the Court deemed "a method of organizing human activity"—*Alice*'s "concept of intermediated settlement" was held to be "'a fundamental economic practice long prevalent in our system of commerce.'" *Alice*, 134 S. Ct. at 2356. Similarly, the Court found that "[t]he use of a third-party intermediary . . . is also a building block of the modern economy." *Id*. "Thus," the Court held, "intermediated settlement . . . is an 'abstract idea' beyond the scope of § 101." *Id*.

2. DataTreasury's Challenged Claims Contain an Abstract Idea

a. Transferring information from one location to another where the transferred information is unreadable without a secret decoder key

Independent claim 43 is illustrative and directed to a system for central management, storage, and report generation of remotely captured paper transactions. Ex. 1002, 28:28–45. Claim 43 requires a remote data access subsystem for capturing and sending the paper transaction data, a central data processing subsystem for processing, sending, verifying and storing the paper transaction data and at least one communication network for transmission of the transaction data. Additionally, claim 43 also requires a data access subsystem providing encrypted subsystem identification information and encrypted paper transaction data to the data processing subsystem. As apparent from claim 43, and identified in the Decision on Institution, Patent Owner's claims are, in substance, directed to the underlying idea of transferring information from one location to another where the transferred information is unreadable without a secret decoder key. Dec. on Inst., 17.

Patent Owner contends that the challenged claims do not recite an abstract idea. Patent Owner argues that, unlike the algorithms in *Benson*, encryption is patent eligible. For example, Patent Owner states:

> Encryption of data as a security measure is, in general, ubiquitous, and differs considerably from a mere mathematical algorithm or formula, and is accomplished not only in the '137 Patent, but is also accomplished in many patents, as discussed above. Class 705, Data Processing: Financial, Business

> Practice, Management, or Cost/Price Determination, includes a large number of patents that encrypt data in subclass 50 and subclasses that are indented under subclass 50.

PO Resp. 53. The fact that other patents have issued that relate to encrypted data fails to demonstrate that the basic concept of encryption is not abstract. An invention is not rendered ineligible for patent simply because it involves an abstract concept. *See Diamond* v. *Diehr*, 450 U. S. 175, 187 (1981).

We agree with Patent Owner that the basic concept of encryption is ubiquitous. Encryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years. Like hedging, encryption in its simplest form does not require the use of technology to communicate secure messages. Specifically, encryption, in its simplest form, could be performed with pencil and paper.

Patent Owner contends that there is no indication that patents employing encryption have been held to recite an abstract idea. PO Resp. 55. Patent Owner relies upon *TQP Development, LLC v. Intuit Inc*., No. 2:12-CV-180, 2014 WL 651935 (E.D. Tex. Feb. 19, 2014), for the proposition that a general recitation of encryption renders the claims patent eligible and that encryption is not an abstract idea. PO Resp. 56, 62–63.

The *TQP* decision concerns a motion for summary judgment of invalidity of U.S. Patent No. 5,412,730, which alleged that the asserted claims were invalid as directed to patent-ineligible subject matter. *TQP*, 2014 WL 651935, at *3. Claim 1, the only asserted

independent claim, related to a method of transmitting encrypted data. The method included the steps of providing a sequence of blocks in encrypted form by providing a seed value to a transmitter and a receiver, generating a first sequence of a pseudo-random key value based on the seed value, and encrypting the data sent. Additionally, the method required the generation of a second sequence of pseudo-random key values that are produced at a time dependent upon predetermined characteristics of the data transmitted, and decrypting the data in accordance with the second sequence. *Id*. at *1–*2.

The district court in *TQP* characterized the asserted claims as directed to a "statutory process" under section 101 and proceeded to the question of whether the recited claim raised "abstractness" problems, which the court characterized as posing a risk of preempting an abstract idea. *Id*. at 6. On this point, the court stated:

> Because the claim language is generic in nature—referring to a "transmitter," a "receiver," and a "communication link," rather than more specific structures, there would appear to be some risk of unacceptable preemption.

Id. Where a risk exists, the court stated that a determination needed to be made as to whether the claims contained additional substantive limitations such that, in practical terms, the claims do not cover the full abstract idea itself. *Id*. at *5–*6. The court reviewed the claims and held that they were drawn to a very specific encryption method, added required steps to the core idea underlying the invention, and involved a way of making computer communication itself more effective by making that communication more secure. *Id*. at *7–*14. Further, the court determined that the motion for summary judgment

raised factual issues. *Id*. at *10. Based on its review, the court denied the motion for summary judgment.

We hold, as did the court in *TQP*, that the challenged claims pose a risk of unacceptable preemption as the claim language is generic in nature—referring to capturing images, managing the transaction data, collecting the data, encrypting subsystem identification information and transaction data, verifying data and transmitting data within and between a remote location and a central location. Accordingly, we review the claims for an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the ineligible concept itself. *Mayo*, 132 S. Ct. at 1294.

b. Imaging or scanning documents

Patent Owner attempts to recast the identified abstract idea by focusing on the imaging and scanning concepts encompassed by the challenged claims. For example, Patent Owner states:

> With respect to §101, the real issue in this CBM Proceeding is whether the teaching of scanning or imaging of documents and receipts is an "abstract idea."

PO Resp. 46. While we have identified the abstract idea as involving the transfer of information from one location to another where the transferred information is unreadable without a secret decoder key, we address Patent Owner's arguments concerning the abstractness of imaging and scanning to the extent the arguments may be of general applicability.

i. Routine business practices can be abstract

Patent Owner contends that the imaging of documents and receipts is not an abstract idea or concept. PO Resp. 33. According to Patent Owner, "[i]maging or scanning a check or other financial document is a routine practice in the business of banking/financial matters" and that routine practices are not abstract. *Id*. Patent Owner also states that scanning or imaging a document is not an abstract idea contending "[i]nstead, it is a practice that is essentially universal, especially in business environments such as banking or financial businesses." *Id*. at 36. For example, Patent Owner states:

> It borders on the absurd to believe that the widespread process of imaging or scanning a check and extracting data from the check is an "abstract idea."

Id. at 51. The fact that a business practice is used widely does not preclude a determination that the underlying practice involves an abstract idea. For instance, risk hedging (*Bilski*) and intermediated settlement (*Alice*) are also routine business practices, but these practices have been held abstract.

ii. Presence of tangible objects does not foreclose abstractness

Patent Owner contends that imaging or scanning a check is not an abstract idea because documents and receipts are concrete objects. *Id*. at 49. The fact that a claim recites substantial physical limitations does not preclude a determination that the claim is effectively an unpatentable law of nature or an attempt to preempt an abstract idea. *Mayo*, 132 S. Ct. at 1297.

3. DataTreasury's Challenged Claims Do Not Contain Significant Meaningful Limitations Beyond the Abstract Idea

Petitioner contends that the '137 patent claims, when considered as a whole, fail to add anything significant to the underlying abstract idea. Pet. 22. Specifically, Petitioner states that the challenged claims add only well-known computer and imaging components in connection with the commonly-known multiple "tier" architecture. *Id*. at 22–23.

Petitioner identifies claim 43 as representative and states that the claim merely recites a method comprising the steps of capturing a check image, sending the image within and between various locations within a system, encrypting subsystem identification information and verifying the check transaction data. *Id*. at 24. Petitioner relies upon the testimony of Dr. Peter Alexander to support its contention that the claim adds nothing more than an arrangement of generic computer components and processes that were known to those of ordinary skill in the art, to the underlying abstract idea. Ex. 1003 ¶¶ 31–77, 104–138.

Patent Owner disagrees, and contends that claim 43 recites specific structural components that are cooperating subsystems that transmit data within and between one or more remote subsystems. PO Resp. 60–61. Patent Owner states that the combination of subsystem components and the three-tiered architecture banking/financial system are simply not taught or suggested in the prior art. *Id*. at 63.

Claim 43 is representative of the challenged claims. The apparatus and method steps recited in claim 43 do not limit the claim in a meaningful way to avoid unacceptable preemption of the abstract idea. Patent Owner

acknowledges that scanning or imaging checks is a "fundamental process" that is performed in a large number of different systems and that such imaging or scanning is a function that has been performed by banking or financial institutions for many years. *Id*. at 63–64, 66. Patent Owner recognizes that encryption of data as a security measure is, in general, "ubiquitous." *Id*. at 53. Patent Owner also acknowledges that the subsystems recited in the challenged claims are composed of "off the shelf" technology. *Id*. at 12–13. Patent Owner also states that the '137 patent discusses a number of hardware options but that the claims do not claim any "particular" machines or components, as the invention is in the configuration of the system. Prelim. Resp. 27–28.

As to the "three-tier" architecture,[2] Dr. Alexander testifies that such architecture was known in the art. For example, Dr. Alexander cites U.S. Patent No. 5,373,550 to Campbell (Exhibit 1023), as describing tiered architecture with imaged checks being routed through network, such as that recited in the challenged claims. Ex. 1003, ¶¶ 208–215. Patent Owner acknowledges that the Campbell patent cited by Dr. Alexander was old and well known long prior to the issue date of the involved patent. PO Resp., 15. We credit Dr. Alexander's testimony and find that three-tier architecture was conventional in the banking and financial services industry.

We credit Dr. Alexander's testimony and determine that the '137 patent simply arranges old well-known elements with each performing the

[2] Petitioner contends that the challenged claims do not recite a "three-tiered" architecture. Reply, 8. For purposes of this decision, we assume the Patent Owner is correct in stating that its claims require such architecture.

same function it had been known to perform. *E.g.*, Ex. 1003 ¶¶ 26–28, 31, 85. Based on the record presented, we do not see how the limitations in claim 43 are significant meaningful limitations that transform the abstract idea into patent-eligible applications of these abstractions. Patent Owner's contentions focus on the alleged meaningful limitations appearing in claim 43 or the challenged claims in general. We have reviewed the remaining challenged claims and are likewise persuaded, based on the evidence presented, that the remaining claims also lack limitations that meaningfully limit the abstract idea and avoid unacceptable preemption. Reply 1. We hold that the challenged claims recite nothing more than conventional equipment and steps, specified at a high level of generality on top of the underlying abstract concept. *Mayo*, 132 S. Ct. at 1300.

We note that Patent Owner states that imaging or scanning a document would transform the paper document into an image on film, or into data, and would satisfy the machine-or-transformation test. PO Resp. 36–37. Patent Owner however, also states that the machine-or-transformation test "does not have any applicability in this proceeding." *Id*. at 35. The challenged claims as a whole, however, do not result in any transformed articles. Rather, transaction (financial) data are duplicated, organized, and moved from one place to another. Ex. 1003 ¶¶ 139–141. Further, the fact that the claims involve the use of generic, well-known machines does not impart patentability under the machine-or-transformation test. *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972) (invalidating as patent-ineligible claimed processes that "can be carried out in existing computers long in use, no new machinery being necessary"). Simply appending conventional steps, specified at a high level of generality is not enough to

supply an inventive concept and transform and otherwise patent-ineligible abstract idea into a patent-eligible subject matter.

We hold that the additional limitations in Patent Owner's claims that seek to narrow the application of the abstract idea are merely an attempt to limit the use of the abstract idea to a particular field of use or add token postsolution components, which has long been held insufficient to save a claim in this context. *See Alice*, 134 S. Ct. at 2358; *Mayo*, 132 S. Ct. at 1294; *Bilski*, 561 U.S. at 610–11; *Diehr*, 450 U.S. at 191. We hold that Petitioner has shown by a preponderance of the evidence that claims 1–67 of the '137 patent are unpatentable under 35 U.S.C. § 101.

D. Grounds Based on 35 U.S.C. § 112, 1st Paragraph, Written Description—Claims 1–67

Petitioner contends that claims 1–67 are unpatentable under 35 U.S.C. 112, first paragraph, written description, because the '137 patent specification lacks sufficient disclosure that would have indicated to one of ordinary skill in the art that patentee possessed the claimed invention. Pet. 38–49. In particular, Petitioner contends that the '137 patent specification fails to describe "encrypting subsystem identification information." *Id*. at 39–46. Specifically, independent claims 1 and 26 require two different types of encrypted information: 1) encrypted paper transaction data, and 2) encrypted subsystem identification information. According to Petitioner, the '137 patent specification discloses that a compressed bitmap image (CBI) is encrypted (ECBI) and that a tag is prepended to the ECBI to form a tagged encrypted compressed bitmap image (TECBI). Pet. 40. Petitioner states that the '137 patent specification suggests that the tag prepended to the ECBI remains unencrypted. Pet. 40–41. Petitioner, and Dr. Alexander, conclude

that the specification suggests that that subsystem identification information remains unencrypted. Pet. 40; Ex. 1003, ¶¶ 143, 149–158, 183. Patent Owner disagrees. PO Resp. 66–72.

Patent Owner directs our attention to column 8, lines 10–30 of the '137 patent specification,[3] which describes encrypting the compressed bitmap image to form an ECBI. PO Resp. 68. Patent Owner also directs our attention to column 11, lines 9–15 of the specification, which provides that the DataTreasury System 100 can process receipts with alternate form as long as the receipt contains the appropriate information. *Id*. at 68–69. Patent Owner, from these cited passages, states that it is clear that one of ordinary skill in the art would understand that the specification supports the encrypting subsystem identification information claim limitation. *Id*. at 69. Specifically, Patent Owner concludes that:

> One of ordinary skill in the art would certainly understand that the "identification information" discussed in those portions of the specification discussed above relate to information that is not only all about a particular subsystem, but instead is information about a transaction engaged in by a person. "Encrypting subsystem identification information" is a claim limitation indicating that data about "identification information," as that term is defined in the original specification of the '137 Patent, is ultimately encrypted in a subsystem of the overall system.

PO Resp. 70.

[3] For purposes of this decision we assume that the cited portions of the '137 patent specification appear verbatim in the originally filed specification of U.S. Application No. 09/081,012, from which the '137 patent issued.

The test for written description is an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art. Using this test, the invention must be described in a manner sufficient to demonstrate that the inventor actually invented the claimed invention. *Ariad Pharm. Inc. v. Eli Lilly & Co.*, 598 F.3d 1336 (Fed. Cir. 2010). "One shows that one is 'in possession' of the invention by describing the invention, with all its claimed limitations, not that which makes it obvious." *Lockwood v. Am. Airlines, Inc.*, 107 F.3d 1565, 1571 (Fed. Cir. 1997). Written description is a question of fact judged as of the relevant filing date. *Falko-Gunter Falkner v. Inglis*, 448 F.3d 1357, 1363 (Fed. Cir. 2006).

The claims require encrypting "subsystem identification information" and not merely "identification information." Patent Owner's citations to the '137 patent specification fail to demonstrate that Patent Owner possessed the invention. As recognized by Dr. Alexander, one skilled in the art would understand that the '137 patent specification does not describe any encryption to the tag headers that are prepended to the ECBI. Ex. 1003 ¶¶ 149–159. Specifically, the '137 patent specification discloses a data access terminal (DAT) having a scanner that is used to scan a financial document, such as a receipt, to create a bitmap image of the document, which can then be compressed. Ex. 1002, 7:59–67, Fig. 2. The specification states that the DAT can use well-known encryption algorithms to encrypt the compressed bitmapped image. *Id*. at 8:10–12. The specification further discloses that once the ECBI has been generated, a tag is prepended to the ECBI to form the TECBI. *Id*. at 8:21–24. This process of forming a TECBI

is depicted in Figure 3A, which provides a flowchart of the process with the tag being added after the ECBI has been encrypted.

Based on the evidence of record, we credit the testimony of Dr. Alexander and agree with Petitioner that:

> (1) the specification fails to describe encrypting the DAT_TERMINAL_ID;
> (2) generic "identification information" does not constitute the claimed subsystem identification information; and
> (3) subsystem identification information is not included in the "paper transaction data" of the disclosed receipt.

Reply 12–13. We find that Petitioner has demonstrated that claims 1–67 are unpatentable for lack of sufficient written description for encrypting subsystem identification information.

III. CONCLUSION

We conclude Petitioner has proven, by a preponderance of the evidence, that claims 1–67 of the '137 patent are unpatentable under 35 U.S.C. § 101; and, that claims 1–67 of the '137 patent are unpatentable under 35 U.S.C. § 112, first paragraph, for lack of written description.

IV. ORDER

For the reasons given, it is hereby:

ORDERED that Petitioner has established by a preponderance of the evidence that claims 1–67 of the ’197 patent are unpatentable;

FURTHER ORDERED that because this is a Final Written Decision, parties to the proceeding seeking judicial review of the Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

CBM 2014-00020
Patent 6,032,137

For PETITIONER:

Erika H. Arner, Lead Counsel
Darren M. Jiron, Backup Counsel
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.
11955 Freedom Drive
Reston, VA 20190
E-Mail: Erika.Arner@finnegan.com
E-Mail: Darren.Jiron@finnegan.com
Telephone 571-203-2700

For PATENT OWNER:

Abraham Hershkovitz, Lead Counsel
Eugene C. Rzucidlo, Backup Counsel
HERSHKOVITZ & ASSOCIATES, PLLC
2845 Duke Street
Alexandria, VA 22314
E-Mail AHershkovitz@Hershkovitz.net
E-Mail GRzucidlo@Hershkovitz.net
Telephone 703-370-4800

Trials@uspto.gov
571-272-7822

Paper 13
Entered: April 29, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FIDELITY NATIONAL INFORMATION SERVICES, INC.,
Petitioner,

v.

DATATREASURY CORP.,
Patent Owner.

Case CBM2014-00020
Patent 6,032,137

Before MICHAEL P. TIERNEY, WILLIAM V. SAINDON, and MATTHEW R. CLEMENTS, *Administrative Patent Judges*.

TIERNEY, *Administrative Patent Judge*.

DECISION
Institution of Covered Business Method Patent Review
37 C.F.R. § 42.208

I. INTRODUCTION

Fidelity National Information Services, Inc. ("Fidelity" or "Petitioner") filed a petition ("Pet.") on October 25, 2013 to institute a covered business method patent review of claims 1-67 of U.S. Patent No. 6,032,137 (Ex. 1002, "the '137 patent"). Paper 2. DataTreasury Corp. ("Patent Owner" or "DataTreasury") filed a preliminary response ("Prelim. Resp.") to the petition on February 1, 2014. We have jurisdiction under 35 U.S.C. § 324. *See* Section 18(a) of the Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284, 329 (2011) ("AIA").

The standard for instituting a covered business method patent review is set forth in 35 U.S.C. § 324(a), which provides as follows:

> THRESHOLD.—The Director may not authorize a post-grant review to be instituted unless the Director determines that the information presented in the petition filed under section 321, if such information is not rebutted, would demonstrate that it is more likely than not that at least 1 of the claims challenged in the petition is unpatentable.

Upon consideration of the information presented, we grant the petition, because Petitioner has demonstrated that claims 1-67 are more likely than not unpatentable under 35 U.S.C. § 101 and unpatentable under 35 U.S.C. § 112 for lack of written description.

A. Related Proceedings

Petitioner indicates that the '137 patent is asserted in a litigation titled *DataTreasury Corp. v. Fidelity National Information Services, Inc.*, No. 2:13-cv-432 (E.D. Tex). Pet. 16. Petitioner also identifies an additional twenty-three district court proceedings involving the '137 patent. Pet. 4-6.

B. The '137 Patent (Ex. 1002)

The '137 patent is directed to a system for remote data acquisition, and centralized processing and storage of the acquired data. Ex. 1002, Abstract. An object of the invention is to provide an automated system to manage and store captured electronic and paper transactions from various activities including banking and consumer applications. *Id*. at 3:22-26. Generally, the '137 patent describes scanning documents using a scanner attached to a general purpose network computer that is connected via a carrier cloud to a server that inserts images and data received into a database. *Id*. at Figs. 1-2, 3:37-58, 4:65-5:15, 5:45-51, 16:53-60. Additionally, the general purpose network computer encrypts the images and data to provide a system with maximal security. *Id*. at 3:30-36, 7:38-46, 8:10-15.

Figure 1 of the '137 patent, provided below, depicts a preferred embodiment of the system having three major operational elements:

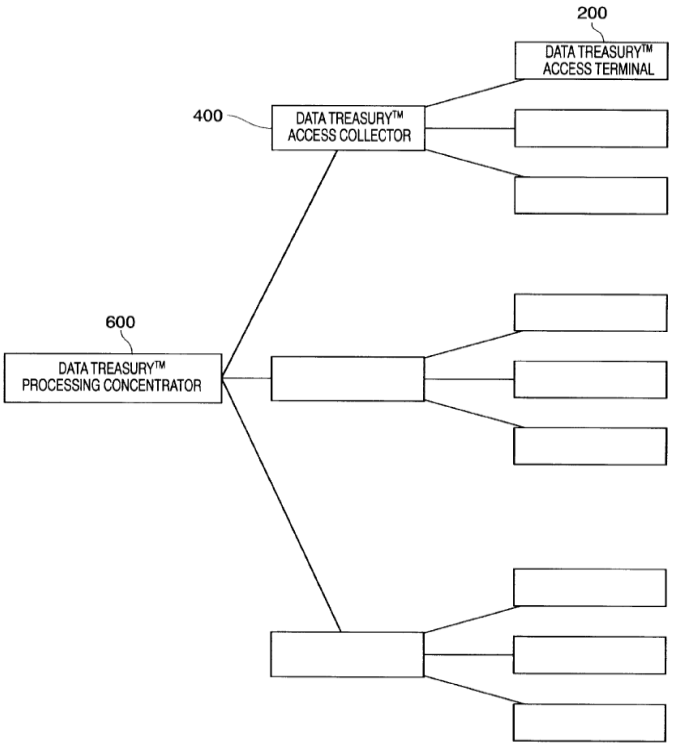


FIG. 1

The ’137 patent describes the tiered arrangement depicted in Figure 1 as follows:

> FIG. 1 shows the architecture of the DataTreasury™ System 100. The DataTreasury™ System 100 has three operational elements: the DataTreasury™ System Access Terminal (DAT) 200 (the remote data access subsystem), the DataTreasury™ System Access Collector (DAC) 400 (the intermediate data collecting subsystem), and the DataTreasury™ System Processing Concentrator (DPC) 600 (the central data processing subsystem).

Id. at 4:66-5:6.

Figure 2 of the ’137 patent, provided below, depicts a block diagram of the DAT (remote data access subsystem terminal):

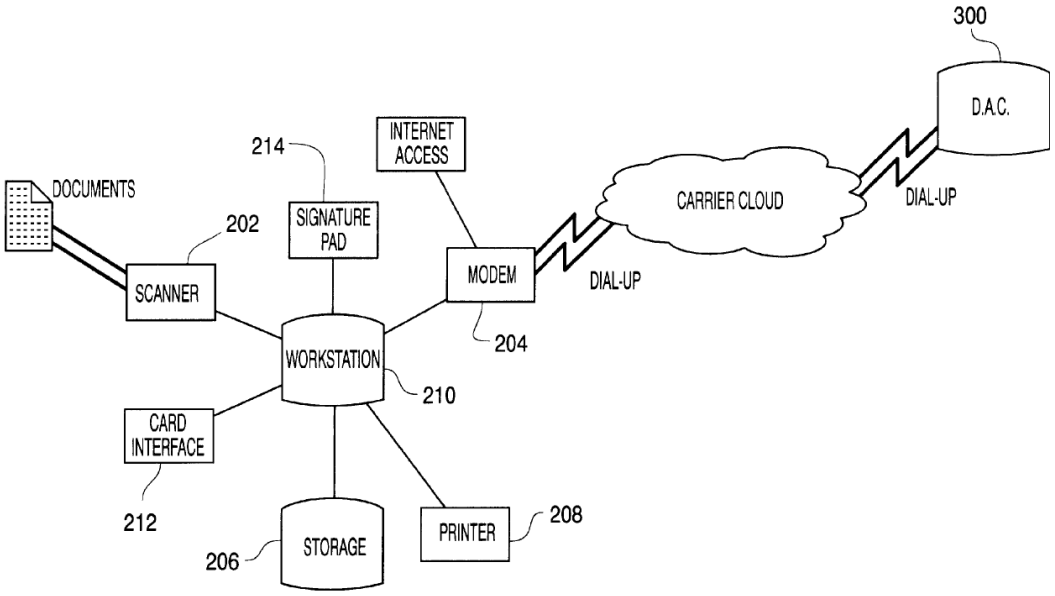


FIG. 2

As shown in Figure 2, scanner 202 is connected to workstation 210, which is connected to data system access collector 300. The workstation can be a general purpose computer and performs tasks including compressing, encrypting, and tagging a scanned bitmapped image. *Id*. at 5:40-45, 7:31-35.

The '137 patent is said to improve upon the prior art by providing an automated, reliable, secure system to process electronic and paper transactions. *Id*. at 3:32-37.

C. Exemplary Claims

Independent claims 26 and 42 are representative of the challenged claims in the '137 patent and are reproduced below:

> 26. A method for central management, storage and verification of remotely captured paper transactions from checks comprising the steps of:
>
> capturing an image of the paper transaction data at one or more remote locations including a payer bank's identification number, a payer bank's routing number, a payer bank's routing information, a payer's account number, a payer's check, a payer

bank's draft, a check amount, a payee bank's identification information, a payee bank's routing information, and a payee's account number; and sending a captured images of the transaction data;

managing the capturing and sending of the transaction data;

collecting, processing, sending and storing the transaction data at a central location;

managing the collecting, processing, sending and storing of the transaction data;

encrypting subsystem identification information and the transaction data; and

transmitting the transaction data and the subsystem identification information within and between the remote location(s) and the central location.

42. A system for central management, storage and report generation of remotely captured paper transactions from checks comprising:

one or more remote data access subsystems for capturing and sending paper transaction data and verifying transaction data from the checks comprising at least one imaging subsystem for capturing the checks and at least one data access controller for managing the capturing and sending of the transaction data;

at least one central data processing subsystem for processing, sending, verifying and storing the paper transaction data and the subsystem identification information comprising a management subsystem for managing the processing, sending and storing of the of the transaction data; and

at least one communication network for the transmission of the transaction data within and between said one or more data access subsystems and said at least one data processing subsystem, with the data access subsystem providing encrypted subsystem identification information and encrypted paper transaction data to the data processing subsystem.

D. The Asserted Grounds

Petitioner contends that the challenged claims are unpatentable based on the following grounds:

Grounds	Claims Challenged
§ 112, Written Description	1-67
§ 101	1-67

II. ANALYSIS

A. Claim Construction

Consistent with the statute and legislative history of the AIA, the Board interprets claims of an unexpired patent using the broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.300(b); *see also* Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,766 (Aug. 14, 2012). Moreover, claim terms are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art at the time of the invention and in the context of the patent disclosure. *In re Translogic Tech., Inc*., 504 F.3d 1249, 1257 (Fed. Cir. 2007). An inventor may rebut the presumption that claim terms are given their ordinary and customary meaning by providing a definition of the term in the specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

Petitioners seek construction of two claim terms. Pet. 17-20. Patent Owner did not propose alternate constructions.

1. "Encrypt" or "Encrypting" (claims 1, 4, 5, 26, 27, 42, and 43)

The claim term "encrypt" or "encrypting" is recited in claims 1, 4, 5, 26, 27, 42, and 43. Petitioner proposes that encrypt or encrypting be construed as "convert into a form unreadable by anyone without a secret

decryption key." Pet. 19. (citing Ex. 1003, Declaration of Dr. Peter Alexander[1] ¶¶ 84, 85).

The '137 patent describes its encryption algorithm as one that would be well known to an artisan of ordinary skill. Ex. 1002 at 8:10-12. In previous district court litigation, "encrypt" was construed to mean "transformation of data into a form unreadable by anyone without a secret decryption key." Ex. 1017, 58-59. Dr. Alexander, however, testifies that the broadest reasonable construction would not be limited to taking action on "data." Ex. 1003 ¶ 86. Dr. Alexander also testifies that encryption must keep the content the same, even though the resulting form may be different, and thus, the underlying information is not transformed as required by the district court construction. Ex. 1003, ¶ 87.

Based upon the record presented, we credit Dr. Alexander's Declaration and, for purposes of this Decision to Institute for the '137 patent, adopt Petitioner's proposed construction.

2. "Within and Between" (claims 1, 26, 42, and 43)

The claim term "within and between" is recited in claims 1, 26, 42, and 43. Petitioner contends that the broadest reasonable interpretation of this terminology is data is transmitted both within a given subsystem (i.e., between the various components comprising the subsystem or location) and between one subsystem or location to another subsystem or location. Pet. 19-20. Petitioner's proposed claim construction is identical to the District Court's Claim Construction Order in *DataTreasury Corp. v. Wells Fargo &*

[1] We conclude that Dr. Alexander is qualified to testify as to the understanding of one skill in the art in this proceeding. *See* Ex. 1003 ¶¶ 1-4.

Co., No: 2:05-cv-291 (E.D. Tex. Mar. 11, 2009). Dr. Alexander testifies that the District Court's construction is consistent with the plain meaning as understood by one of ordinary skill in the art. Ex. 1003 ¶¶ 92, 94-95.

Based upon the record presented, we credit Dr. Alexander's Declaration and, for purposes of this Decision to Institute for the '137 patent, adopt the District Court's proposed construction, which is advanced by the Petitioner.

B. Standing for Covered Business Method Review of the '137 Patent

The parties disagree as to whether Petitioner has standing to file a petition for a covered business method review of the '137 patent. *See* Pet. 7-17; Prelim. Resp. 7-14. Section 18 of the AIA provides for the creation of a transitional program for reviewing covered business method patents. A "covered business method patent" is a patent that "claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service, except that the term does not include patents for technological inventions." AIA § 18(d)(1); *see* 37 C.F.R. § 42.301(a). To determine whether a patent is eligible for a covered business method patent review, the focus is on the claims. *See* Transitional Program for Covered Business Method Patents—Definitions of Covered Business Method Patent and Technological Invention; Final Rule, 77 Fed. Reg. 48,734, 48,736 (Aug. 14, 2012). A patent need have only one claim directed to a covered business method to be eligible for review. *Id*.

1. Sued for Infringement of the '137 Patent

The AIA requires that "[a] person may not file a petition for a transitional proceeding unless the person or the person's real party in interest or privy has been sued for infringement of the patent or has been charged with infringement under that patent." AIA § 18(a)(1)(B); *see also* 37 C.F.R. § 42.302(a).

As discussed above, Petitioner represents that it has been sued for infringement of the '137 patent in *DataTreasury Corp. v. Fidelity National Information Services, Inc.*, No. 2:13-cv-432 (E.D. Tex). Thus, Petitioner has been sued for infringement for purposes of AIA § 18(a)(1)(B).

2. Financial Product or Service

A "covered business method patent" is a patent that "claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service, except that the term does not include patents for technological inventions." AIA § 18(d)(1); *see* 37 C.F.R. § 42.301(a) (emphasis added).

In promulgating rules for covered business method reviews, the Office considered the legislative intent and history behind the AIA's definition of "covered business method patent." *See* Transitional Program for Covered Business Method Patents—Definitions of Covered Business Method Patent and Technological Invention; Final Rule, 77 Fed. Reg. 48,734, 48,735-36 (Aug. 14, 2012). The "legislative history explains that the definition of covered business method patent was drafted to encompass patents 'claiming activities that are financial in nature, incidental to a financial activity or complementary to a financial activity.'" *Id*. (citing 157 Cong. Rec. S5432

(daily ed. Sept. 8, 2011) (statement of Sen. Schumer)). The legislative history indicates that "financial product or service" should be interpreted broadly. *Id*.

The '137 patent describes capturing an image of financial transaction data, including sale, business, banking, and general consumer transactions, and transmitting the image to a storage facility, where the information about the financial transaction is recorded and stored. Ex. 1002, Abstract, 3:30-57. For example, claim 26 is directed to a "method for central management, storage and verification of remotely captured paper transactions from checks." We determine that such activity falls within a financial product or service as it is directed to a financial activity, namely processing financial transactions (checks).

Based on the foregoing, the '137 patent claims methods that are directed to a financial activity—processing financial transactions—that constitutes a financial product or service under § 18(d)(1).

3. Technological Invention

The definition of "covered business method patent" in Section 18(d)(1) of the AIA excludes patents for "technological inventions." In determining whether a patent is for a technological invention, we consider "whether the claimed subject matter as a whole recites a technological feature that is novel and unobvious over the prior art; and solves a technical problem using a technical solution." 37 C.F.R. § 42.301(b). The following claim drafting techniques, for example, typically do not render a patent a "technological invention":

> (a) Mere recitation of known technologies, such as computer hardware, communication or computer networks, software, memory, computer-readable storage medium,

> scanners, display devices or databases, or specialized machines, such as an ATM or point of sale device.
>
> (b) Reciting the use of known prior art technology to accomplish a process or method, even if that process or method is novel and non-obvious.
>
> (c) Combining prior art structures to achieve the normal, expected, or predictable result of that combination.

Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,763-64 (Aug. 14, 2012).

Petitioner contends that the '137 patent claims fail to recite a novel and unobvious technological feature. Pet. 11-14. Patent Owner disagrees and states that the '137 patent is directed to a technological data processing system that performs a technological method driven by that technological data processing system. Prelim. Resp. 12.

We exercise our discretion and analyze claim 26 of the '137 patent to determine whether it recites a novel and unobvious technological feature. Claim 26 is directed to a method for central management, storage and verification of remotely captured paper transactions from checks. The method requires the steps of capturing an image of the paper transaction data, where the image may be captured using a conventional scanner. The transaction data are transferred from a remote location. The transaction data are managed, collected, processed, sent, and stored at a central location. The subsystem identification information and transaction data are then encrypted, which can be done using a conventional algorithm. The transaction data and subsystem identification information are transmitted within and between the remote location and central location. None of the steps in claim 26 recites a novel and unobvious technological feature. Ex. 1003 ¶¶ 105-111. This is consistent with the description in the '137 patent specification and

confirmed by the inventor of the '137 patent, who testified in a trial before the District Court that he did not actually create hardware when he came up with the invention. Ex. 1013, 63:15-24.

Based on the foregoing, we conclude that claim 26 of the '137 patent is not a technological invention under § 18(d)(1). Additionally, we conclude that the '137 patent is eligible for a covered business method patent review.

C. Grounds Based on 35 U.S.C. § 112, 1st Paragraph, Written Description—Claims 1-67

Petitioner contends that claims 1-67 are unpatentable under 35 U.S.C. 112, 1st paragraph, written description, because the '137 patent specification lacks sufficient disclosure that would have indicated to one of ordinary skill in the art that patentee possessed the claimed invention. Pet. 38-49.

The test for written description is an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art. Using this test, the invention must be described in a manner sufficient to demonstrate that the inventor actually invented the claimed invention. *Ariad Pharm. Inc. v. Eli Lilly & Co*., 598 F.3d 1336 (Fed. Cir. 2010). "One shows that one is 'in possession' of the invention by describing the invention, with all its claimed limitations, not that which makes it obvious." *Lockwood v. Am. Airlines, Inc*., 107 F.3d 1565, 1571 (Fed. Cir. 1997).

1. Encrypted/Encrypting Subsystem Identification Information

Petitioner contends that claims 1-67 are unpatentable for lack of written description. Pet. 38-46. Specifically, independent claims 1 and 26 require two different types of encrypted information: 1) encrypted paper transaction data, and 2) encrypted subsystem identification information.

According to Petitioner, the '137 patent specification discloses that a compressed bitmap image (CBI) is encrypted (ECBI) and that a tag is prepended to the ECBI to form a tagged encrypted compressed bitmap image (TECBI). Pet. 40. Petitioner states that the '137 patent specification suggests that the tag prepended to the ECBI remains unencrypted. Pet. 40-41. Patent Owner disagrees, contending that encrypting subsystem information refers to encrypting identification information, such as that found on a sales receipt. Prelim. Resp. 41-45.

Dr. Alexander testifies that one skilled in the art would understand that the '137 patent specification does not describe any encryption to the tag headers that are prepended to the ECBI. Ex. 1003 ¶¶ 149-159. Specifically, the '137 patent specification discloses a data access terminal (DAT) having a scanner that is used to scan a financial document, such as a receipt, to create a bitmap image of the document, which can then be compressed. Ex. 1002, 7:59-67, Fig. 2. The specification states that the DAT can use well-known encryption algorithms to encrypt the compressed bitmapped image. *Id*. at 8:10-12. The specification further discloses that once the ECBI has been generated, a tag is prepended to the ECBI to form the TECBI. *Id*. at 8:21-24. This process of forming a TECBI is depicted in Fig. 3A, which provides a flowchart of the process with the tag being added after the ECBI has been encrypted.

Patent Owner contends that one skilled in the art would understand that "encrypting subsystem identification information" is directed to encrypting "identification information," such as the transaction data, which is scanned and converted to an ECBI. The claims, however, require encrypting "subsystem identification information" and not merely

"identification information."

Based on the record presented, we credit Dr. Alexander's testimony and find that Petitioner has demonstrated that claims 1-67 are more likely than not unpatentable for lack of sufficient written description for encrypting subsystem identification information.

2. Within and Between

Petitioner contends that claims 1-67 are unpatentable as the claim term "within and between" lacks sufficient written description. Pet. 46-49. Petitioner states that the '137 patent specification does not describe the transmission of data within subsystems of the same hierarchical level. Pet. 49. Petitioner cites Dr. Alexander's Declaration for support.

The term "within and between" appears in the Summary of the Invention portion of the '137 patent specification at col. 3, ll. 55-58. We find that Petitioner has failed to demonstrate that claims 1-67 are more likely than not unpatentable for lack of sufficient written description for the term "within and between."

D. Grounds Based on 35 U.S.C. § 101— Claims 1-67 Directed to Non-Statutory Subject Matter

Petitioner contends that claims 1-67 are unpatentable under 35 U.S.C. § 101, because they are directed toward ineligible subject matter. Pet. 20-37. Petitioner relies on the Declaration of Dr. Alexander (Ex. 1003 ¶¶ 104-141) to support its contention that the challenged claims are unpatentably abstract and fail the machine-or-transformation test. *Id*.

Patent Owner asserts that there is nothing "abstract" about encryption of data through the use of software, the transmission of data between locations or subsystems, and the imaging of a document. Prelim. Resp.

25-30. In particular, Patent Owner asserts that the encryption cannot be abstract as there is no mathematical encryption formula disclosed in the '137 patent specification, especially since the '137 patent refers to the use of well-known encryption algorithms. *Id*. Patent Owner further asserts that the claims of the '137 patent are directed to a system and that the various system components that might be used in constructing the claimed system are mere examples and "preferred embodiments" rather than absolute requirements. Prelim. Resp. 34. Given that the claims are directed to a system, Patent Owner contends that Petitioner has failed to consider the claims as a whole.

On the present record, we determine that Petitioner has shown that claims 1-67 are more likely than not unpatentable under 35 U.S.C. § 101.

The Supreme Court has made it clear that the test for patent eligibility under § 101 is not amenable to bright-line categorical rules. *See Bilski v. Kappos*, 130 S. Ct. 3218 (2010); *see also Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 132 S. Ct. 1289 (2012). Section 101 provides that "[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title." The plain language of the statute and use of the term "any" shows that "Congress contemplated that the patent laws would be given wide scope" for patent eligible subject matter. *Bilski v. Kappos*, 130 S. Ct. 3218, 3225 (2010) (quoting *Diamond v. Chakrabarty*, 447 U.S. 303, 308 (1980)). Accordingly, there are three limited, judicially created exceptions to the broad categories of patent-eligible subject matter in Section 101: laws of nature, natural phenomena, and abstract ideas. *Mayo*, 132 S. Ct. at 1293.

An abstract idea by itself is not patentable, but a practical application of an abstract idea may be deserving of patent protection. *Id*. at 1293-94; *see Bilski*, 130 S. Ct. at 3230; *Diamond v. Diehr*, 450 U.S. 175, 187 (1981). To be patent-eligible, a claim must incorporate enough meaningful limitations to ensure that it claims more than just an abstract idea and is not merely a "drafting effort designed to monopolize the [abstract idea] itself." *Mayo*, 132 S. Ct. at 1297. Limiting the claim to a particular technological environment or field of use, or adding insignificant pre- or post-solution activity, do not constitute meaningful limitations. *See Bilski*, 130 S. Ct. at 3230; *Diehr*, 450 U.S. at 191-92; *Parker v. Flook*, 437 U.S. 584, 595 n.18 (1978).

The subject matter of claims 1-67, when considered as a whole, is directed to an abstract idea; namely, the underlying idea of transferring information from one location to another where the transferred information is unreadable without a secret decoder key. Here, the use of private encrypted messages communicated from one location to another represent a "disembodied concept," a basic building block of human ingenuity. Thus, we analyze the claims to determine if they "incorporate enough meaningful limitations to ensure that the claims cover more than just an abstract idea." *See Mayo*, 132 S. Ct. at 1297.

Claim 43 is representative of the challenged claims. Claim 43 is directed to a method comprising capturing an image of a check, collecting, managing, encrypting, and verifying the data from the check, and transmitting the data to various locations within a system. Claim 43 does not require particular apparatus that limit the claim in a meaningful way. Dr. Alexander testifies that the '137 patent simply arranges old well-known

elements with each performing the same function it had been known to perform. Patent Owner does not dispute Dr. Alexander's testimony. For example, Patent Owner states that the '137 patent discusses a number of hardware options but that the claims do not claim any "particular" machines or components, as the invention is in the configuration of the system. Prelim. Resp. 27-28. Based on the record presented, we do not see how the limitations in claim 43 are significant meaningful limitations that transform the abstract idea into patent-eligible applications of these abstractions.

Petitioner identifies how the remaining claims, claims 1-42 and 44-67, also add only routine operations and generic computer components to the abstract idea. Patent Owner does not present separate arguments for its claims. Accordingly, on the present record, we hold that claims 1-42 and 44-67 do not recite significant meaningful limitations on the abstract idea for the same reasons we held that claim 43 does not recite significant meaningful limitations.

Patent Owner contends that its claims do not preempt any abstract idea, as there is nothing abstract about its claimed system and method claims. Prelim. Resp. 30-33. We disagree. The claims do not add meaningful limitations to avoid preempting the basic concept of transferring information from one location to another where the transferred information is unreadable without a secret decoder key. Although the claims are limited to capturing images of paper transaction data, to be meaningful, the claim must contain more than mere field-of-use limitations, tangential references to technology, insignificant pre- or post-solution activity, ancillary data-gathering steps, or the like.

Patent Owner also contends that its claims do not fail the machine-or-transformation test in *Bilski*. Prelim. Resp. 33-41. According to Patent Owner, the particular machine is the claimed system. *Id*. at 33-34. Patent Owner states that a scanner is used to capture an image of the paper transaction data, and that the system thereafter collects, processes, sends, and stores the data. *Id*. The claims as a whole, however, do not result in any transformed articles. Rather, transaction (financial) data are duplicated, organized, and moved from one place to another. Ex. 1003 ¶¶ 139-141. Further, the fact that the claims involve the use of generic, well-known machines does not impart patentability under the machine-or-transformation test. *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972) (invalidating as patent-ineligible claimed processes that "can be carried out in existing computers long in use, no new machinery being necessary").

Based on the foregoing, we are persuaded Petitioner has shown that it is more likely than not that claims 1-67 of the '137 patent are directed toward ineligible subject matter under 35 U.S.C. § 101.

III. CONCLUSION

For the foregoing reasons, we are persuaded that the information presented establishes that it is more likely than not that Petitioner would prevail in establishing the unpatentability of claims 1-67 of the '137 patent.

The Board has not made a final determination on the patentability of any challenged claims.

IV. ORDER

Accordingly, it is

ORDERED that pursuant to 35 U.S.C. § 324(a), the Petition for covered business method patent review is *granted* as to claims 1-67 of the '137 patent on the following grounds:

1. Claims 1-67 as being drawn to non-statutory subject matter under 35 U.S.C. § 101; and
2. Claims 1-67 under 35 U.S.C. § 112, 1st paragraph as lacking sufficient written description for encrypting subsystem identification information.

FURTHER ORDERED that pursuant to 35 U.S.C. § 324(d) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial; the trial commences on the entry date of this decision.

CBM 2014-00020
Patent 6,032,137

For PETITIONER:

Erika H. Arner, Lead Counsel
Darren M. Jiron, Backup Counsel
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.
11955 Freedom Drive
Reston, VA 20190
E-Mail FIS-Ballard@finnegan.com
Telephone 571-203-2700

For PATENT OWNER:

Abraham Hershkovitz, Lead Counsel
Eugene C. Rzucidlo, Backup Counsel
HERSHKOVITZ & ASSOCIATES, PLLC
2845 Duke Street
Alexandria, VA 22314
E-Mail AHershkovitz@Hershkovitz.net
E-Mail GRzucidlo@Hershkovitz.net
Telephone 703-370-4800

US006032137A

United States Patent [19]

Ballard

[11] **Patent Number: 6,032,137**

[45] **Date of Patent: *Feb. 29, 2000**

[54] **REMOTE IMAGE CAPTURE WITH CENTRALIZED PROCESSING AND STORAGE**

[75] Inventor: **Claudio R. Ballard**, Lloyd Harbor, N.Y.

[73] Assignee: **CSP Holdings, LLC**, Lloyd Harbor, N.Y.

[*] Notice: This patent is subject to a terminal disclaimer.

[21] Appl. No.: **09/081,012**

[22] Filed: **May 19, 1998**

Related U.S. Application Data

[63] Continuation-in-part of application No. 08/917,761, Aug. 27, 1997, Pat. No. 5,910,988.

[51] **Int. Cl.**[7] **H04L 9/00**

[52] **U.S. Cl.** **705/75**

[58] **Field of Search** 380/24, 25; 705/75

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,201,978	5/1980	Nally	340/146.3
4,264,808	4/1981	Owens et al.	235/379
4,326,258	4/1982	de la Guardia	364/515
4,417,136	11/1983	Rushby et al.	235/379
4,457,015	6/1984	Nally et al.	382/45
4,523,330	6/1985	Cain	382/7
4,555,617	11/1985	Brooks et al.	235/379
4,680,803	7/1987	Dilella	382/9
4,694,147	9/1987	Amemiya et al.	235/379
4,747,058	5/1988	Ho	364/478
4,750,201	6/1988	Hodgson et al.	379/144
4,843,220	6/1989	Haun	235/380
4,858,121	8/1989	Barber et al.	364/406
4,888,812	12/1989	Dinan et al.	382/7
4,926,325	5/1990	Benton et al.	364/408
4,960,981	10/1990	Benton et al.	235/379
5,091,968	2/1992	Higgins et al.	382/30
5,122,950	6/1992	Benton et al.	364/408
5,144,115	9/1992	Yoshida	235/379
5,159,548	10/1992	Caslavka	364/408
5,173,594	12/1992	McClure	235/380
5,175,682	12/1992	Higashiyama et al.	364/408
5,187,750	2/1993	Behera	382/7
5,204,811	4/1993	Bednar et al.	364/406
5,220,501	6/1993	Lawlor et al.	364/408
5,237,158	8/1993	Kern et al.	235/379
5,274,567	12/1993	Kallin et al.	364/478
5,283,829	2/1994	Anderson	380/24
5,321,238	6/1994	Kamata et al.	235/379
5,321,751	6/1994	Ray et al.	380/23
5,326,959	7/1994	Perazza	235/379
5,345,090	9/1994	Hludzinski	250/566

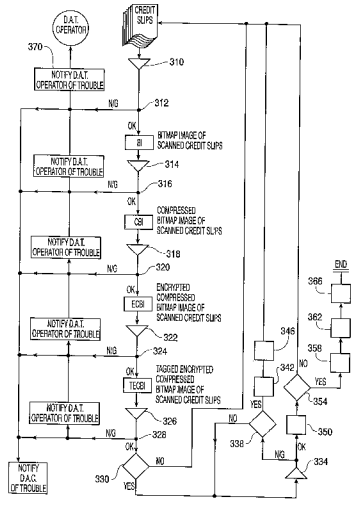
(List continued on next page.)

Primary Examiner—Salvatore Cangialosi
Attorney, Agent, or Firm—J. Michael Martinea de Andino; McGuire, Woods, Battle & Boothe, LLP

[57] **ABSTRACT**

A system for remote data acquisition and centralized processing and storage is disclosed called the DataTreasury™ System. The DataTreasury™ System provides comprehensive support for the processing of documents and electronic data associated with different applications including sale, business, banking and general consumer transactions. The system retrieves transaction data such as credit card receipts checks in either electronic or paper form at one or more remote locations, encrypts the data, transmits the encrypted data to a central location, transforms the data to a usable form, performs identification verification using signature data and biometric data, generates informative reports from the data and transmits the informative reports to the remote location(s). The DataTreasury™ System has many advantageous features which work together to provide high performance, security, reliability, fault tolerance and low cost. First, the network architecture facilitates secure communication between the remote location(s) and the central processing facility. A dynamic address assignment algorithm performs load balancing among the system's servers for faster performance and higher utilization. Finally, a partitioning scheme improves the error correction process.

43 Claims, 11 Drawing Sheets



U.S. PATENT DOCUMENTS

5,434,928	7/1995	Wagner et al.	382/187
5,436,970	7/1995	Ray et al.	380/23
5,444,794	8/1995	Uhland, Sr.	382/137
5,457,747	10/1995	Drexler et al.	380/24
5,479,510	12/1995	Olsen et al.	380/24
5,484,988	1/1996	Hills et al.	235/379
5,506,691	4/1996	Bednar et al.	358/402
5,544,043	8/1996	Miki et al.	364/406
5,590,038	12/1996	Pitroda	395/241
5,602,933	2/1997	Blackwell et al.	382/116
5,604,640	2/1997	Zipf et al.	359/803
5,613,001	3/1997	Bakhoum	380/4
5,647,017	7/1997	Smithies et al.	382/119
5,657,389	8/1997	Houvener	380/23
5,657,396	8/1997	Rudolph et al.	382/190
5,673,333	9/1997	Johnston	382/137
5,751,842	5/1998	Riach et al.	382/137
5,754,673	5/1998	Brooks et al.	382/112
5,781,654	7/1998	Carney	382/137
5,784,503	7/1998	Bleecker, III et al.	382/306
5,787,403	7/1998	Randle	705/43
5,910,988	6/1999	Ballard	380/24

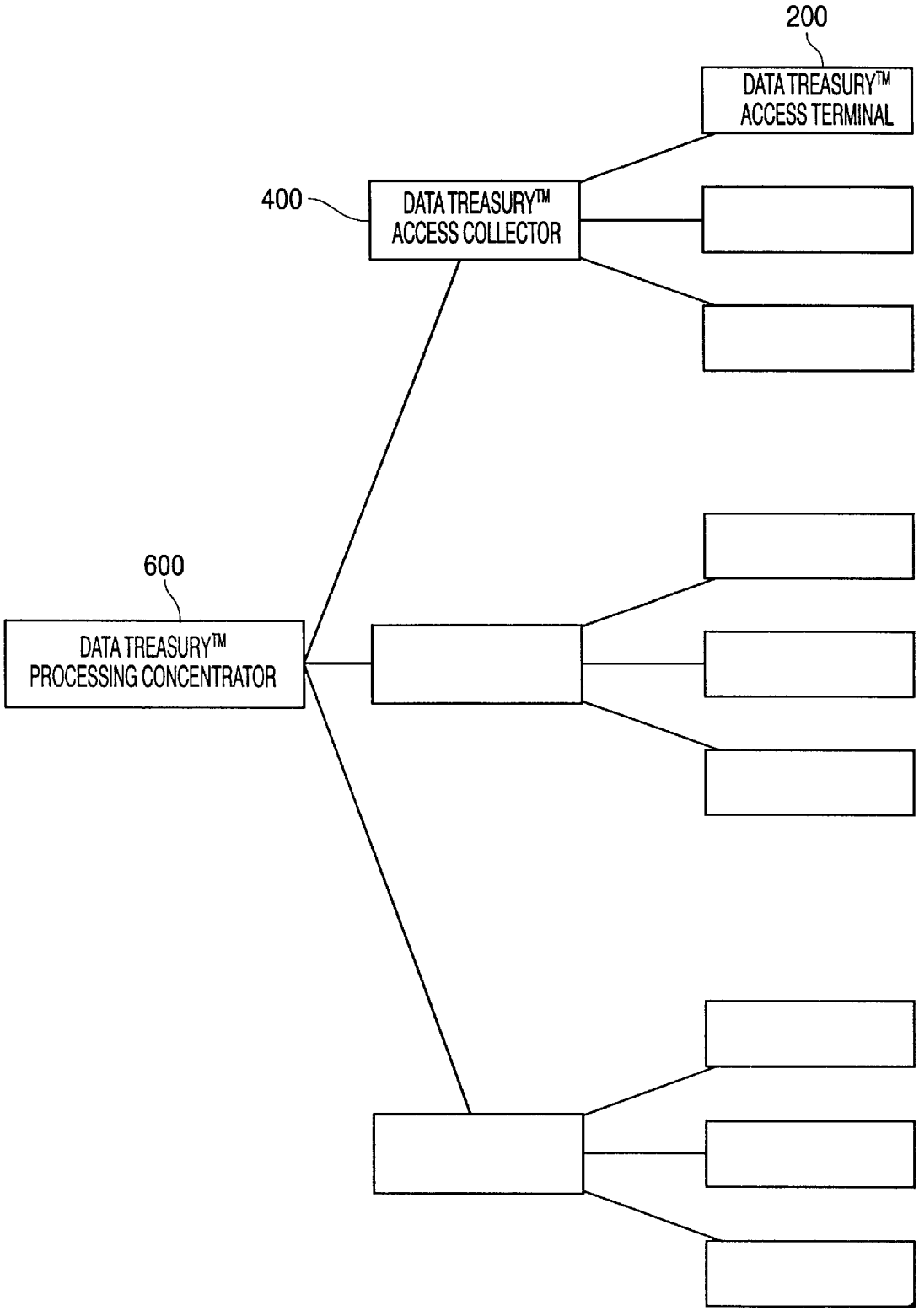

200
DATA TREASURY™ ACCESS TERMINAL
400
DATA TREASURY™ ACCESS COLLECTOR
600
DATA TREASURY™ PROCESSING CONCENTRATOR

FIG. 1

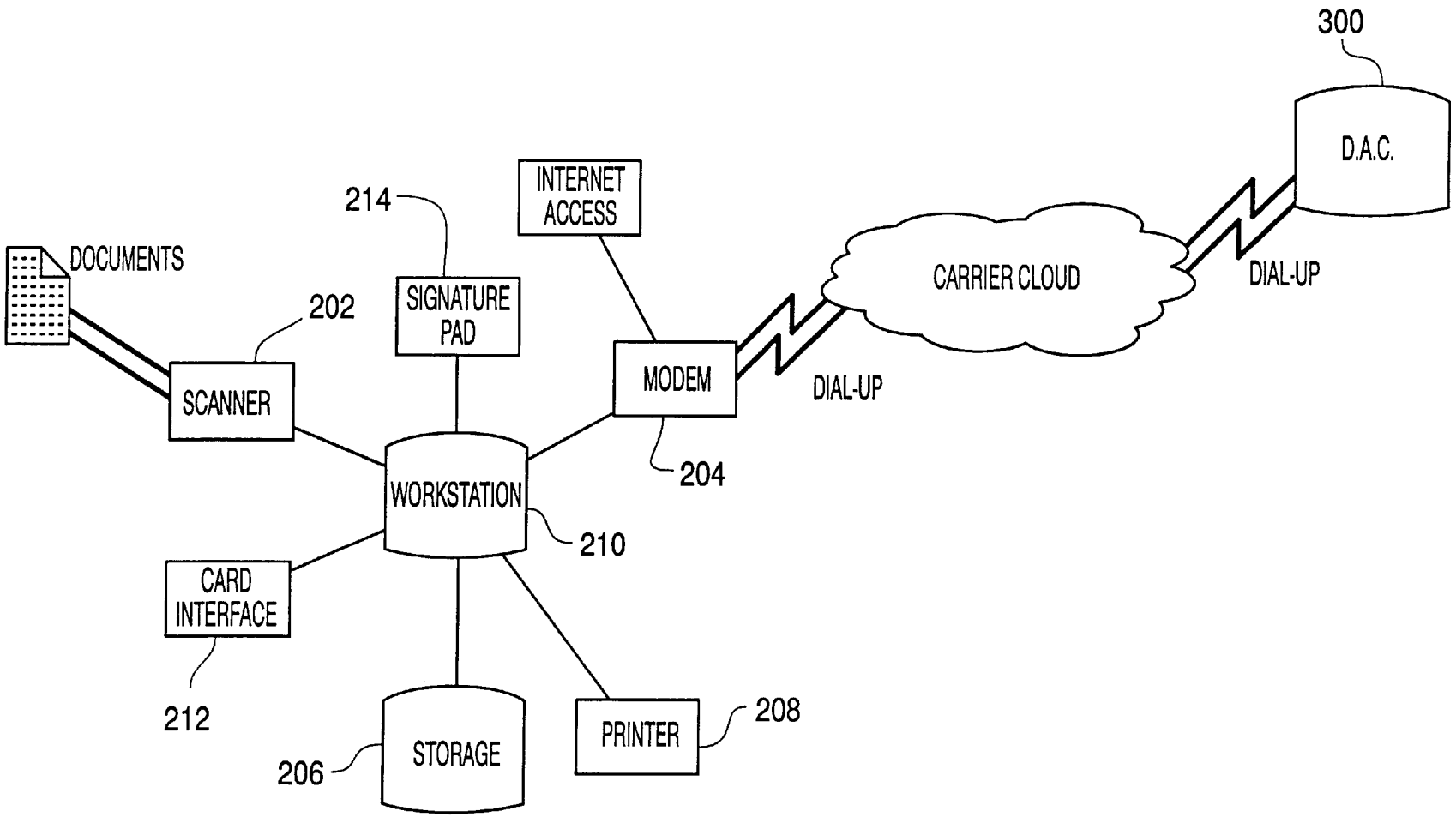

300
D.A.C.
INTERNET ACCESS
214
DOCUMENTS
SIGNATURE PAD
CARRIER CLOUD
DIAL-UP
202
SCANNER
MODEM
DIAL-UP
204
WORKSTATION
210
CARD INTERFACE
212
206
STORAGE
PRINTER
208

FIG. 2

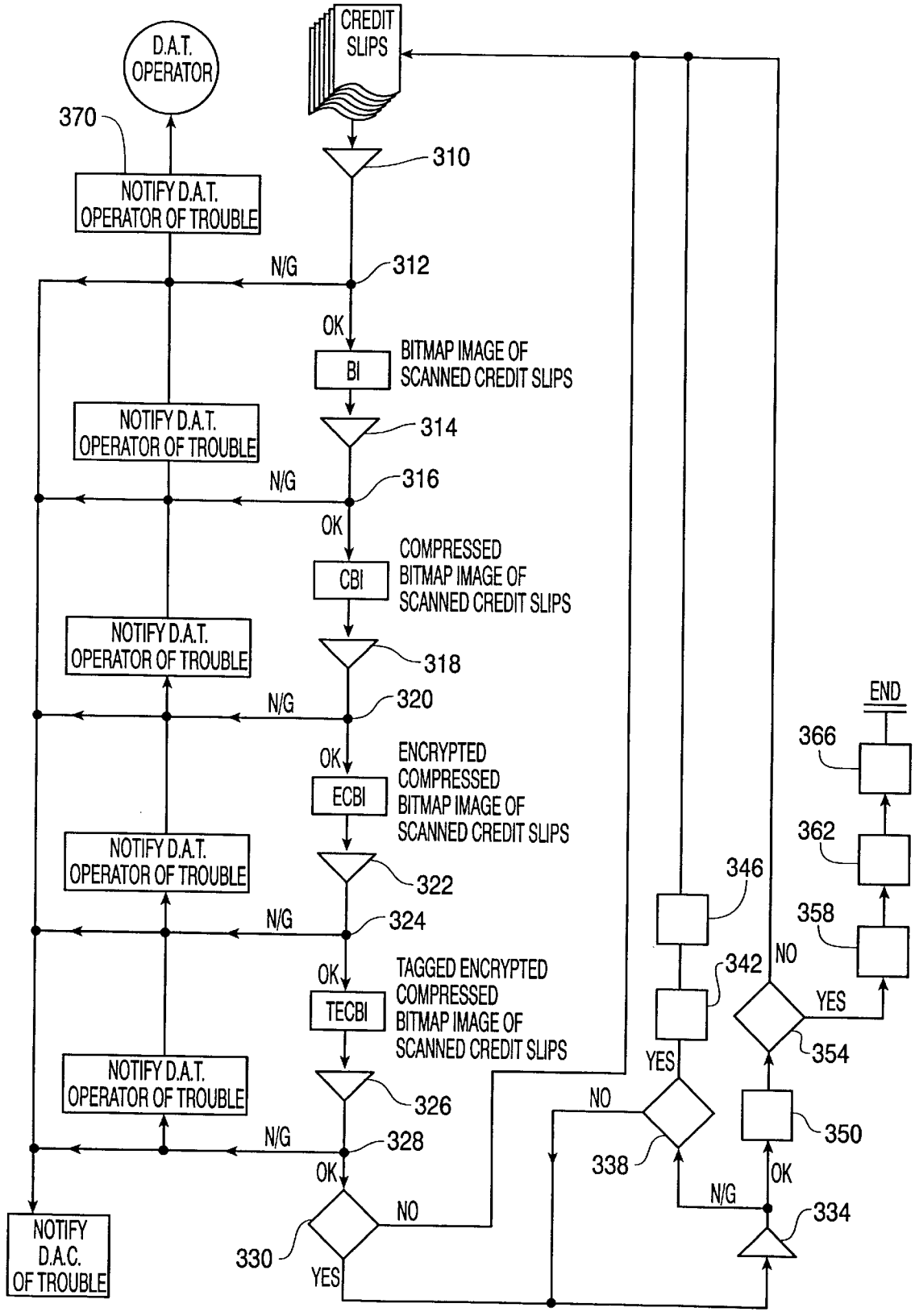

CREDIT SLIPS
D.A.T. OPERATOR
370
310
NOTIFY D.A.T. OPERATOR OF TROUBLE
N/G
312
OK
BI
BITMAP IMAGE OF SCANNED CREDIT SLIPS
NOTIFY D.A.T. OPERATOR OF TROUBLE
314
N/G
316
OK
CBI
COMPRESSED BITMAP IMAGE OF SCANNED CREDIT SLIPS
NOTIFY D.A.T. OPERATOR OF TROUBLE
318
N/G
320
OK
ECBI
ENCRYPTED COMPRESSED BITMAP IMAGE OF SCANNED CREDIT SLIPS
NOTIFY D.A.T. OPERATOR OF TROUBLE
322
N/G
324
OK
TECBI
TAGGED ENCRYPTED COMPRESSED BITMAP IMAGE OF SCANNED CREDIT SLIPS
NOTIFY D.A.T. OPERATOR OF TROUBLE
326
N/G
328
OK
NO
330
YES
NOTIFY D.A.C. OF TROUBLE
346
342
NO
YES
354
YES
NO
338
350
OK
N/G
334
END
366
362
358

FIG. 3A

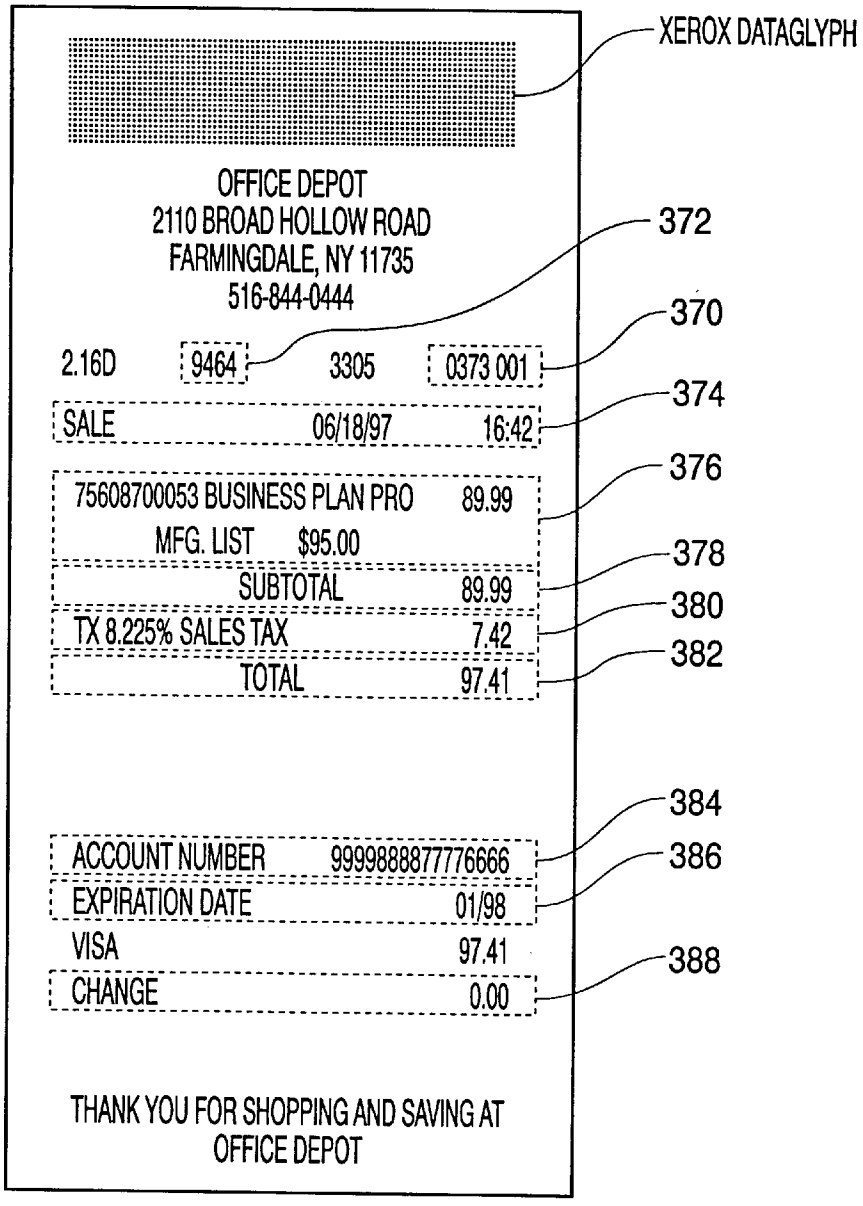

XEROX DATAGLYPH
OFFICE DEPOT
2110 BROAD HOLLOW ROAD
FARMINGDALE, NY 11735
516-844-0444
372
370
2.16D
9464
3305
0373 001
374
SALE
06/18/97
16:42
376
75608700053 BUSINESS PLAN PRO
89.99
MFG. LIST $95.00
378
SUBTOTAL
89.99
380
TX 8.225% SALES TAX
7.42
382
TOTAL
97.41
384
ACCOUNT NUMBER
9999888877776666
386
EXPIRATION DATE
01/98
VISA
97.41
388
CHANGE
0.00
THANK YOU FOR SHOPPING AND SAVING AT
OFFICE DEPOT

FIG. 3B

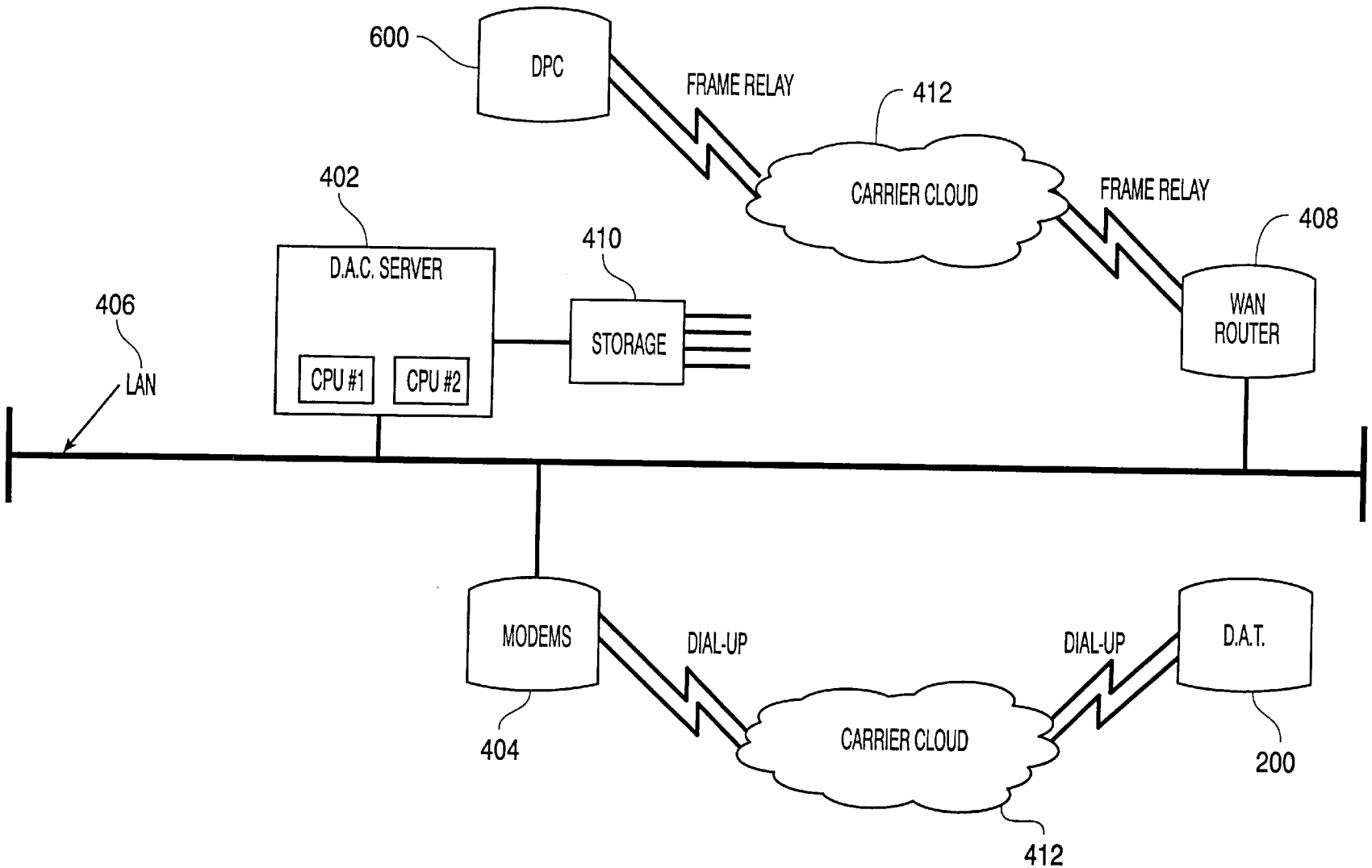

600
DPC
FRAME RELAY
412
CARRIER CLOUD
FRAME RELAY
408
WAN ROUTER
402
D.A.C. SERVER
410
STORAGE
406
LAN
CPU #1
CPU #2
MODEMS
DIAL-UP
DIAL-UP
D.A.T.
404
CARRIER CLOUD
200
412

FIG. 4

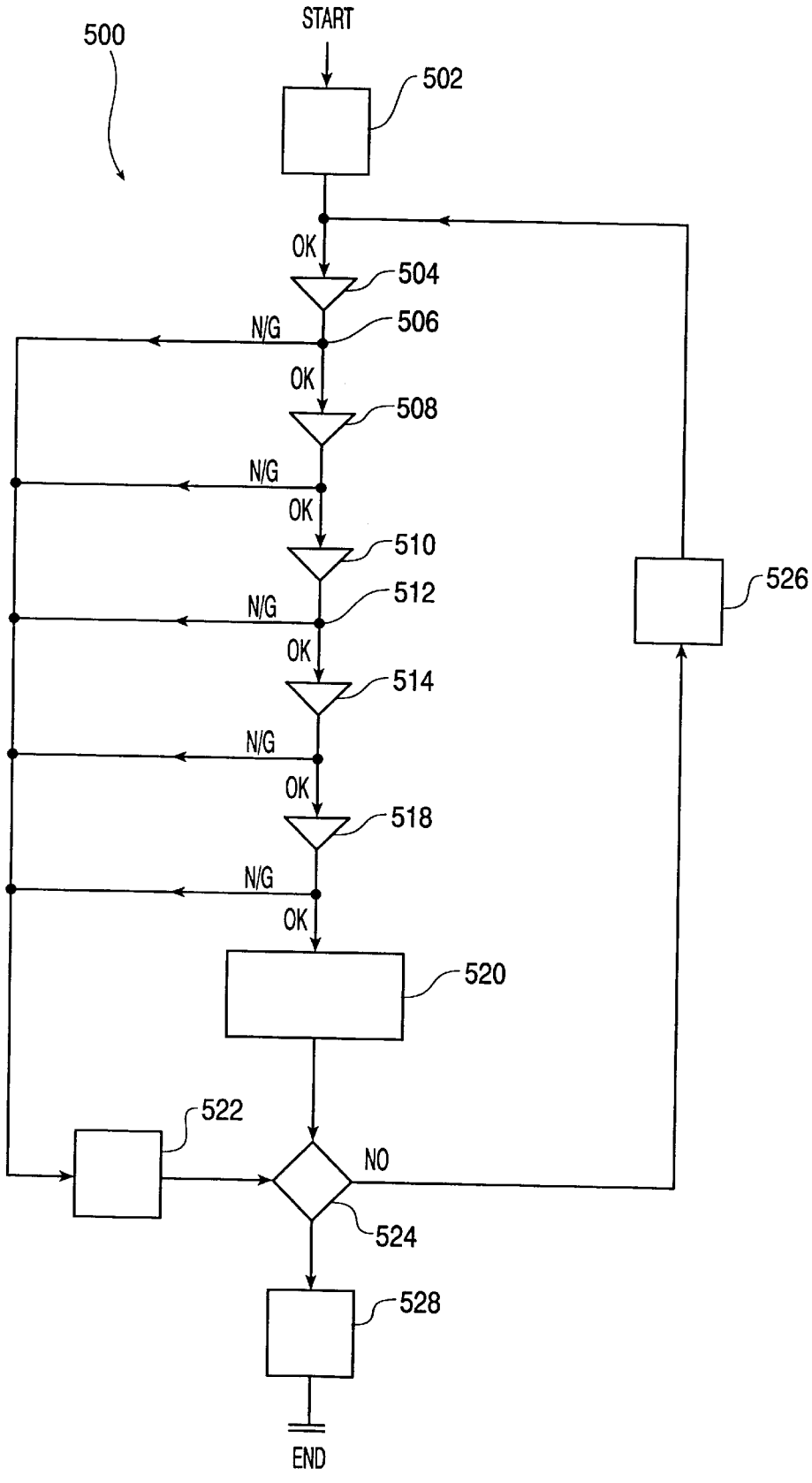

500
START
502
OK
504
N/G
506
OK
508
N/G
OK
510
N/G
512
OK
514
N/G
OK
518
N/G
OK
520
522
NO
524
528
END
526

FIG. 5

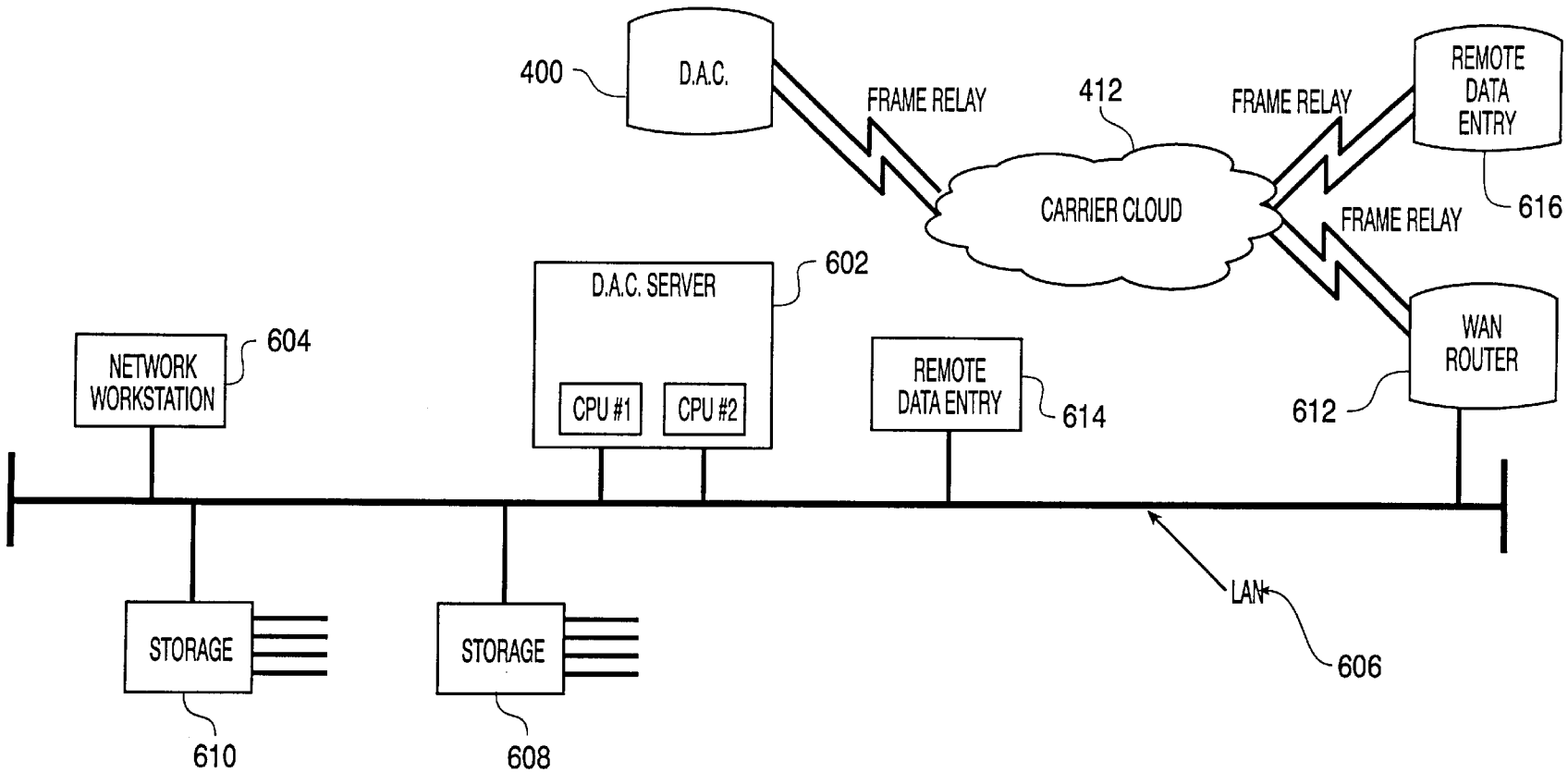

400
D.A.C.
FRAME RELAY
412
CARRIER CLOUD
FRAME RELAY
REMOTE DATA ENTRY
616
FRAME RELAY
WAN ROUTER
612
602
D.A.C. SERVER
CPU #1
CPU #2
604
NETWORK WORKSTATION
REMOTE DATA ENTRY
614
LAN
606
STORAGE
610
STORAGE
608

FIG. 6

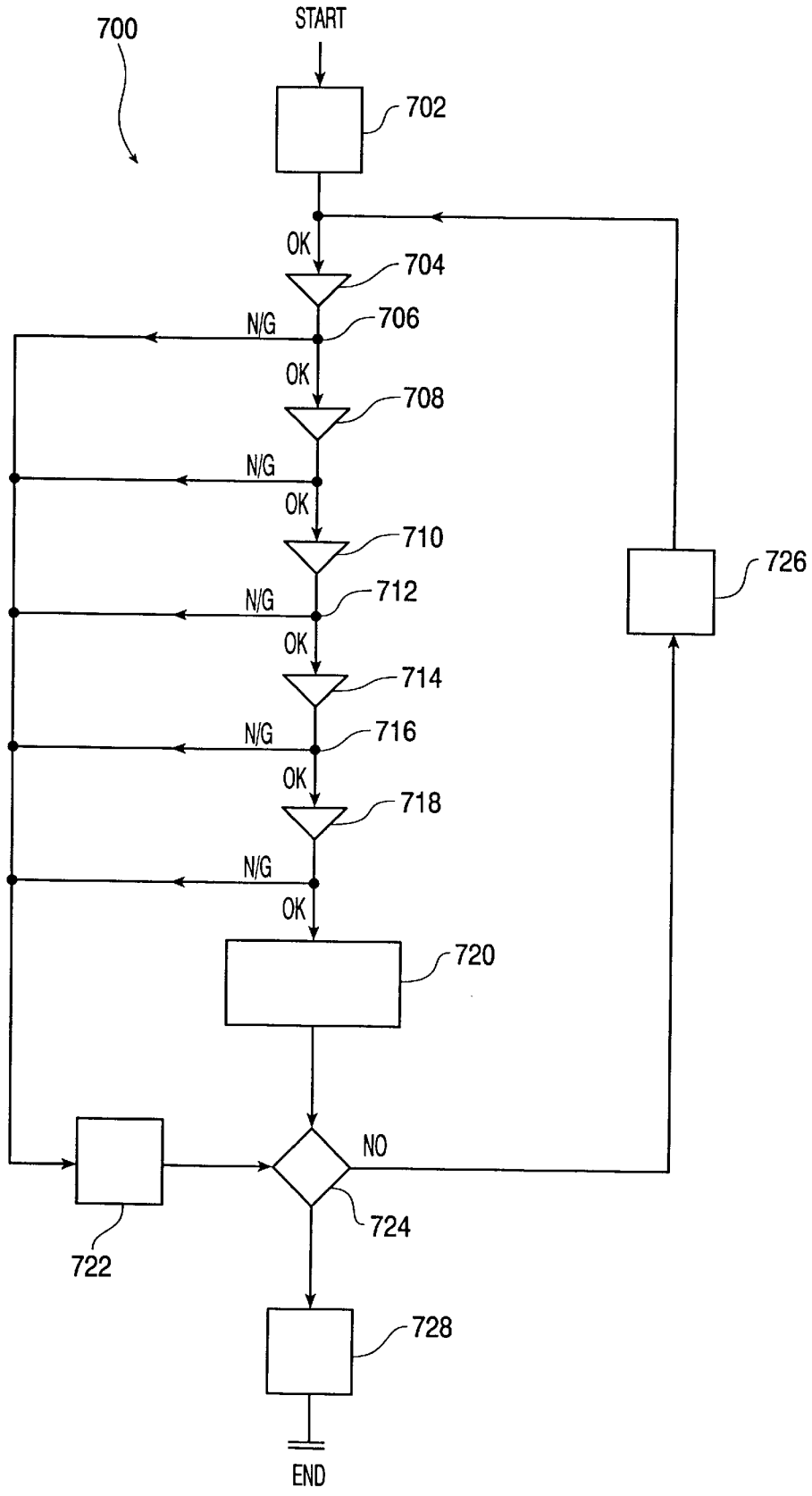

700
START
702
OK
704
N/G
706
OK
708
N/G
OK
710
N/G
712
OK
714
N/G
716
OK
718
N/G
OK
720
726
NO
724
722
728
END

FIG. 7

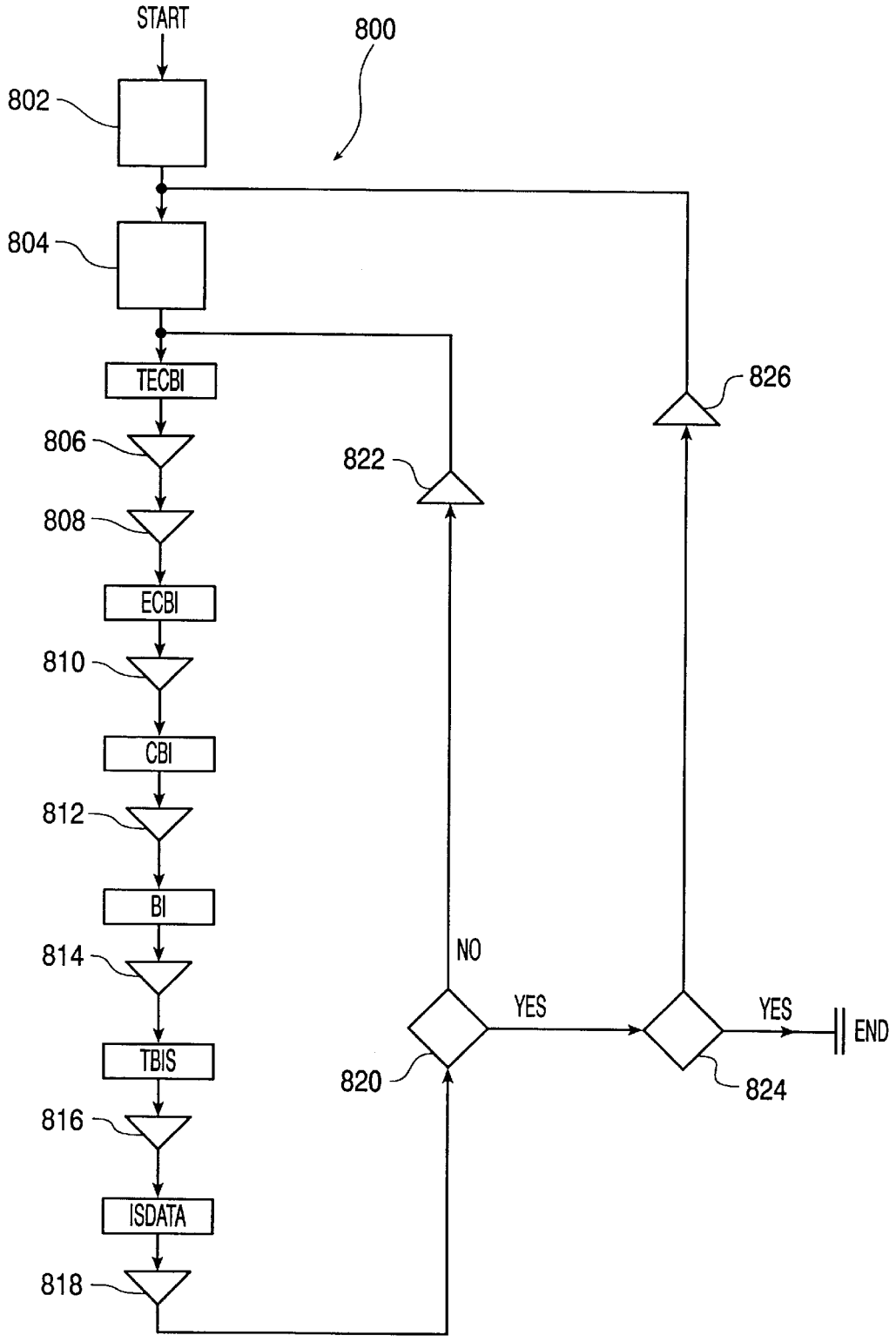

START
800
802
804
TECBI
806
808
ECBI
810
CBI
812
BI
814
TBIS
816
ISDATA
818
822
826
NO
YES
YES
END
820
824

FIG. 8

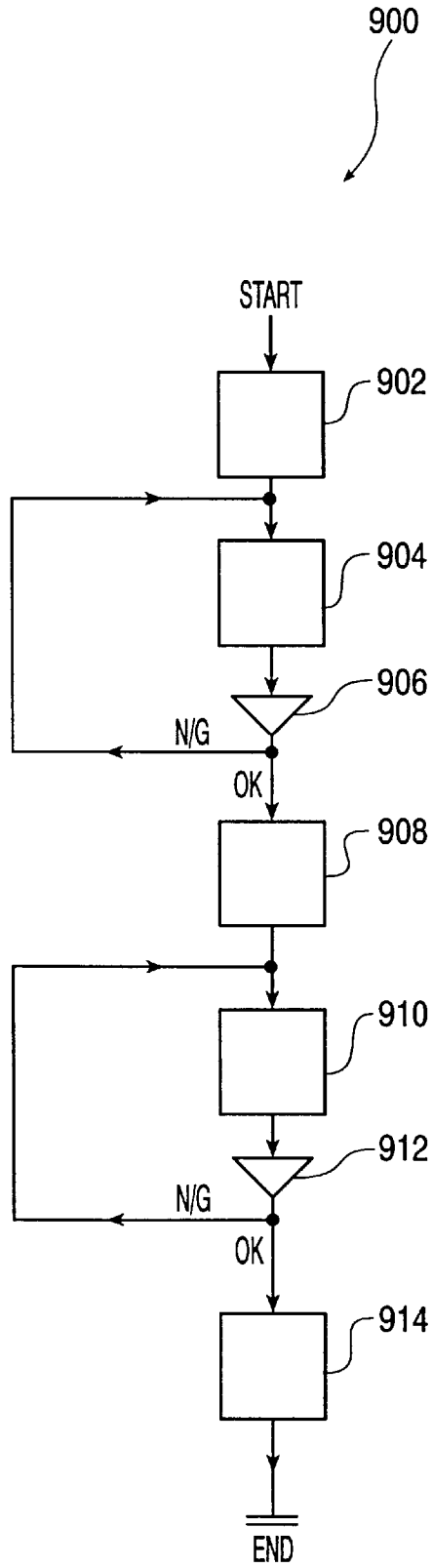


FIG. 9

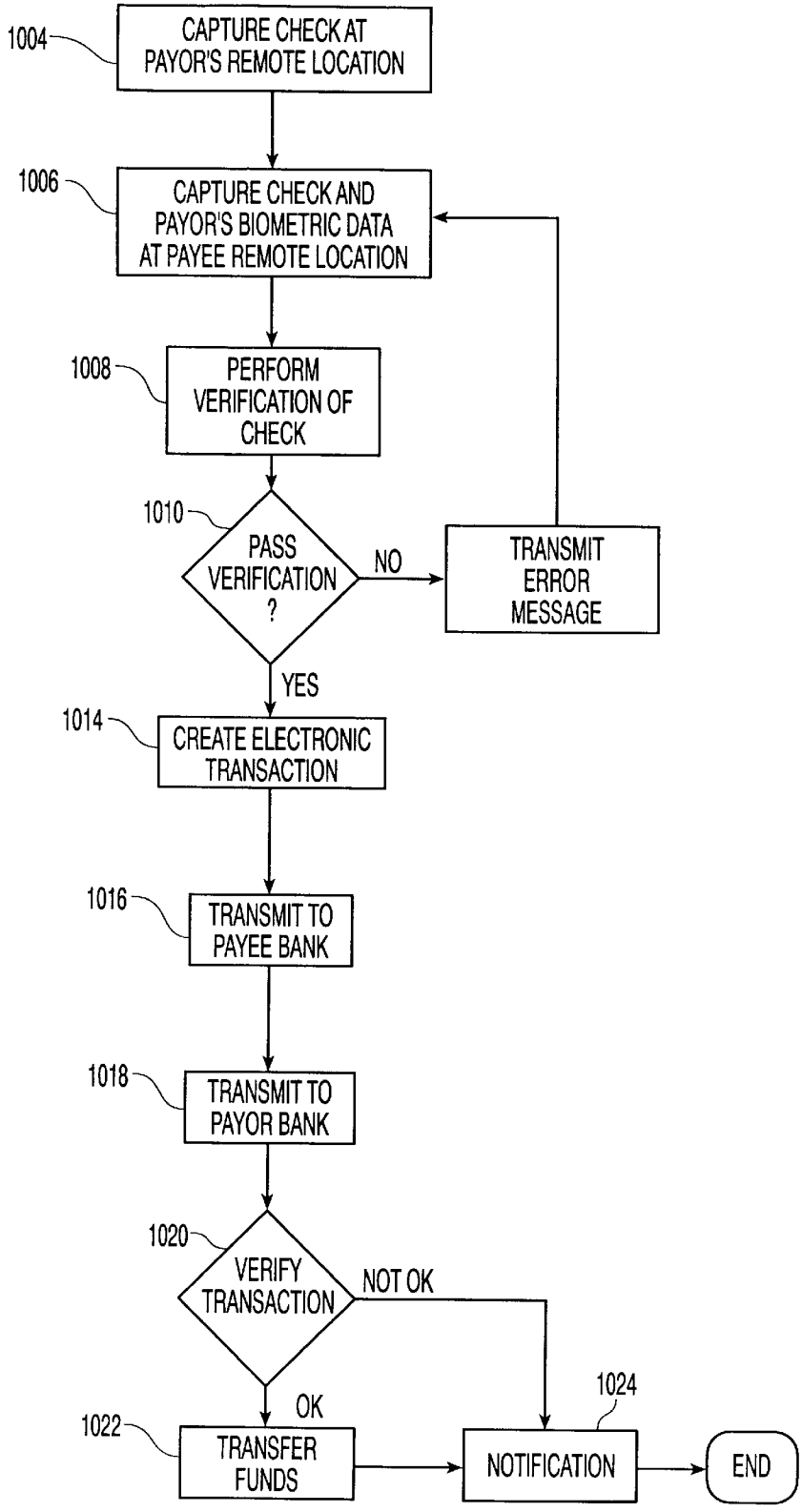

1004
CAPTURE CHECK AT PAYOR'S REMOTE LOCATION
1006
CAPTURE CHECK AND PAYOR'S BIOMETRIC DATA AT PAYEE REMOTE LOCATION
1008
PERFORM VERIFICATION OF CHECK
1010
PASS VERIFICATION ?
NO
TRANSMIT ERROR MESSAGE
YES
1014
CREATE ELECTRONIC TRANSACTION
1016
TRANSMIT TO PAYEE BANK
1018
TRANSMIT TO PAYOR BANK
1020
VERIFY TRANSACTION
NOT OK
OK
1022
TRANSFER FUNDS
1024
NOTIFICATION
END

FIG. 10

REMOTE IMAGE CAPTURE WITH CENTRALIZED PROCESSING AND STORAGE

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation in part of application Ser. No. 08/917,761 filed Aug. 27, 1997, now U.S. Pat. No. 5,910,988.

FIELD OF THE INVENTION

This invention relates generally to the automated processing of documents and electronic data from different applications including sale, business, banking and general consumer transactions. More particularly, it pertains to an automated system to retrieve transaction data at remote locations, to encrypt the data, to transmit the encrypted data to a central location, to transform the data to a usable form, to generate informative reports from the data and to transmit the informative reports to the remote locations.

BACKGROUND

This invention involves the processing of documents and electronic data which are generated, for example, from sale, business and banking transactions including credit card transactions, smart card transactions, automated teller machine (ATM) transactions, consumer purchases, business forms, W2 forms, birth certificates, deeds and insurance documents.

The enormous number of paper and electronic records generated from documents and electronic data from sale, business and banking transactions contain valuable information. First, these paper and electronic records contain information which can be used to verify the accuracy of the records maintained by consumers, merchants and bankers. For example, customers use paper receipts of sale and banking transactions to verify the information on the periodic statements which they receive from their bank or credit card institution. Merchants use paper receipts to record sale transactions for management of customer complaints. Taxpayers use paper receipts to record tax deductible contributions for use in their tax return preparation. Employees use paper receipts to record business expenses for preparation of business expense forms.

Paper and electronic records also contain information which can be used for market analysis. For example, manufacturers and retailers can determine consumer preferences in different regions as well as trends in consumer preferences from the information contained in paper and electronic records.

However, the maintenance and processing of paper and electronic records presents difficult challenges. First, paper receipts and documents could easily be lost, misplaced, stolen, damaged or destroyed. Further, the information contained in these paper and electronic records cannot be easily processed because it is scattered among individual records. For example, the market trend information contained in a group of sales records retained by merchants cannot easily be determined since this information is scattered among the individual records. Likewise, the tax information contained in a group of paper receipts of sales transactions retained by consumers cannot easily be processed.

Previous approaches have been proposed to meet the challenges associated with the maintenance and processing of paper and electronic records. For example, data archive service companies store the information from paper receipts and documents acquired from their customers on microfilm or compact disc read only memory (CD-ROM) at a central facility. Customers typically deliver the paper receipts and documents to the central facility. For sensitive documents which cannot leave the customer site, some data archive service companies perform data acquisition and transfer to magnetic tapes at the customer site and deliver the tapes to the central facility.

The approach offered by these data archive service companies have disadvantages. First, the approach is costly and has poor performance because it requires an expensive, time consuming physical transportation of paper receipts or magnetic tapes from the customer site to the central facility. Further, the approach is not reliable as information can be lost or damaged during physical transportation. The approach also has limited capability as it does not process electronic records along with the paper receipts within a single system.

Other approaches have focused on the elimination of paper receipts and documents. U.S. Pat. No. 5,590,038 discloses a universal electronic transaction card (UET card) or smart card which stores transaction information on a memory embedded on the card as a substitute for a paper receipt. Similarly, U.S. Pat. No. 5,479,510 discloses a method of electronically transmitting and storing purchaser information at the time of purchase which is read at a later time to ensure that the purchased goods or services are delivered to the correct person.

While these approaches avoid the problems associated with paper receipts, they have other disadvantages. First, these approaches do not offer independent verification of the accuracy of the records maintained by consumers, merchants and bankers with a third party recipient of the transaction data. For example, if a UET card is lost, stolen, damaged or deliberately altered by an unscrupulous holder after recording sale or banking transactions, these approaches would not be able to verify the remaining records which are maintained by the other parties to the transactions.

Next, these approaches do not have the ability to process both paper and electronic records of transactions within a single, comprehensive system. Accordingly, they do not address the task of processing the enormous number of paper receipts which have been generated from sales and banking transactions. The absence of the ability to process both paper and electronic records of these approaches is a significant limitation as paper receipts and documents will continue to be generated for the foreseeable future because of concerns over the reliability and security of electronic transactions and the familiarity of consumers and merchants with paper receipts.

These approaches also have a security deficiency as they do not offer signature verification which is typically used on credit card purchases to avoid theft and fraud. For example, a thief could misappropriate money from a UET card holder after obtaining by force, manipulation or theft the user's personal identification number (PIN). Similarly, it is not uncommon for criminals to acquire credit cards in victims' names and make unlawful charges after obtaining the victim's social security number. This becomes a greater concern as that type of personal information becomes available, e.g., on the internet. Also, the signature verification performed manually by merchants for credit card purchases frequently misses forged signatures.

Even if smart cards or UET cards had the ability to store signature and other biometric data within the card for

verification, the system would still have disadvantages. First, the stored biometric data on the card could be altered by a card thief to defeat the security measure. Similarly, the biometric data could be corrupted if the card is damaged. Finally, the security measure would be costly at it would require an expensive biometric comparison feature either on each card or on equipment at each merchant site.

Additional biometric verification systems including signature verification systems have been proposed to address the security problem. For example, U.S. Pat. No. 5,657,393 discloses a method and apparatus for verification of handwritten signatures involving the extraction and comparison of signature characteristics including the length and angle of select component lines. In addition, U.S. Pat. No. 5,602,933 discloses a method and apparatus for the verification of remotely acquired data with corresponding data stored at a central facility.

However, none of these verification systems offer general support for transaction initiation, remote paper and electronic data acquisition, data encryption, data communication, data archival, data retrieval, data mining, manipulation and analytic services. Accordingly, there is a need for a single system which offers comprehensive support for the tasks involved in the automated processing of documents, biometric and electronic data from sale, business, banking and general consumer transactions. Further, there is a need for a single comprehensive system having the reliability, performance, fault tolerance, capacity, cost and security to satisfy the requirements of the retail, business, banking and general consumer industries.

SUMMARY OF THE INVENTION

The invention provides an automated, reliable, high performance, fault tolerant, and low cost system with maximal security and availability to process electronic and paper transactions, and has been named the DataTreasury™ System.

It is an object of the present invention to provide a system for central management, storage and verification of remotely captured electronic and paper transactions from credit cards, smart cards, debit cards, documents and receipts involving sales, business, banking and general purpose consumer applications comprising:

- at least one remote data access subsystem for capturing and sending electronic and paper transaction data;
- at least one data collecting subsystem for collecting and sending the electronic and paper transaction data comprising a first data management subsystem for managing the collecting and sending of the transaction data;
- at least one central data processing subsystem for processing, sending and storing the electronic and paper transaction data comprising a second data management subsystem for managing the processing, sending and storing of the transaction data; and
- at least one communication network for the transmission of the transaction data within and between said at least one data access subsystem and said at least one data processing subsystem.

The DataTreasury™ System processes paper and/or electronic receipts such as credit card receipts, Automated Teller Machine (ATM) receipts, business expense receipts and sales receipts and automatically generates reports such as credit card statements, bank statements, tax reports for tax return preparation, market analyses, and the like.

It is a further object of the DataTreasury™ System to retrieve both paper and electronic transactions at remote locations.

It is a further object of the DataTreasury™ System to employ a scanner and a data entry terminal at a customer site to retrieve data from paper transactions and to enable additions or modifications to the scanned information respectively.

It is a further object of the DataTreasury™ System to provide an input device for retrieving transaction data from the memory of smart cards for independent verification of the records maintained by consumers, merchants and bankers to prevent the loss of data from the loss, theft, damage or deliberate alteration of the smart card.

It is a further object of the DataTreasury™ System to retrieve and process transaction data from DataTreasury™ System anonymous smart cards which are identified by an account number and password. Since DataTreasury™ System anonymous smart card transactions can be identified without the customer's name, a customer can add money to the DataTreasury™ System anonymous smart card and make expenditures with the card with the same degree of privacy as cash acquisitions and expenditures.

It is a further object of the DataTreasury™ System to retrieve customer billing data from employee time documents and to generate customer billing statements from the billing data.

It is a further object of the DataTreasury™ System to initiate electronic transactions including transactions on the internet and to provide identification verification by capturing and comparing signature and biometric data.

It is a further object of the DataTreasury™ System of the invention to process electronic and paper transactions with a tiered architecture comprised of DataTreasury™ System Access Terminals (DATs), DataTreasury™ System Access Collectors (DACs) and DataTreasury™ System Processing Concentrators (DPCs).

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects and features of the invention will be more clearly understood from the following detailed description along with the accompanying drawing figures, wherein:

FIG. **1** is a block diagram showing the three major operational elements of the invention: the DataTreasury™ System Access Terminal (DAT), the DataTreasury™ System Access Collector (DAC) and the DataTreasury™ System Processing Concentrator (DPC);

FIG. **2** is a block diagram of the DAT architecture;

FIG. **3***a* is a flow chart describing image capture by a DAT;

FIG. **3***b* displays a sample paper receipt which is processed by the DAT;

FIG. **4** is a block diagram of the DAC architecture;

FIG. **5** is a flow chart describing the polling of the DATs by a DAC;

FIG. **6** is a block diagram of the DPC architecture;

FIG. **7** is a flow chart describing the polling of the DACs by the DPC;

FIG. **8** is a flow chart describing the data processing performed by the DPC; and

FIG. **9** is a flow chart describing the data retrieval performed by the DPC; and

FIG. **10** is a flow chart describing the use of the DataTreasury™ system to process personal checks.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. **1** shows the architecture of the DataTreasury™ System **100**. The DataTreasury™ System **100** has three

operational elements: the DataTreasury™ System Access Terminal (DAT) **200** (the remote data access subsystem), the DataTreasury™ System Access Collector (DAC) **400** (the intermediate data collecting subsystem), and the DataTreasury™ System Processing Concentrator (DPC) **600** (the central data processing subsystem). The DataTreasury™ System **100** architecture consists of three tiers. At the bottom tier, the DATs **200** retrieve data from the customer sites. At the next tier, the DACs **400** poll the DATs **200** to receive data which accumulates in the DATs **200**. At the top tier, the DPCs **600** poll the DACs **400** to receive data which accumulates in the DACs **400**. The DPCs **600** store the customer's data in a central location, generate informative reports from the data and transmit the informative reports to the customers at remote locations.

In the preferred embodiment, the DataTreasury™ System **100** complies with the Price Waterhouse SAS**70** industry standard. Specifically, the DataTreasury™ System **100** meets the software development standard, the system deployment standard and the reliability standard specified by Price Waterhouse SAS**70**. By adhering to the Price Waterhouse SAS**70** standard, the DataTreasury™ System **100** provides the security, availability and reliability required by mission critical financial applications of banks and stock brokerage companies.

As is known to persons of ordinary skill in the art, the DataTreasury™ System **100** could also use other software development standard, other system deployment standards and other reliability standards as long as adherence to these alternative standards provides the security, availability and reliability required by mission critical financial applications.

FIG. **2** shows a block diagram of the DAT **200** architecture. DATs **200** are located at customer sites. The DataTreasury™ System **100** customers include merchants, consumers and bankers. The DATs **200** act as the customer contact point to the suite of services provided by the DataTreasury™ System **100**. In the preferred embodiment, the DAT **200** is custom designed around a general purpose thin client Network Computer (NC) which runs SUN Microsystem's JAVA/OS operating system. The custom designed DAT **200** comprises a DAT scanner **202**, a DAT modem **204**, DAT digital storage **206**, a DAT controller **210** (workstation), a DAT card interface **212**, an optional DAT printer **208** and a signature pad **214**.

As is known to persons of ordinary skill in the art, the DAT **200** could also be custom designed around a general purpose network computer running other operating systems as long as the chosen operating system provides support for multiprocessing, memory management and dynamic linking required by the DataTreasury™ System **100**.

The DAT scanner **202** scans a paper receipt and generates a digital bitmap image representation called a Bitmap Image (BI) of the receipt. In the preferred embodiment, the DAT scanner **202** has the ability to support a full range of image resolution values which are commonly measured in Dots Per Inch (DPI). Next, the DAT scanner **202** has the ability to perform full duplex imaging. With full duplex imaging, a scanner simultaneous captures both the front and back of a paper document. The DAT scanner **202** can also support gray scale and full color imaging at any bit per pixel depth value. The DAT scanner **202** also supports the capture of handwritten signatures for identity verification.

In addition to scanning images and text, the DAT scanner **202** also scans DataGlyph™ elements, available from Xerox Corporation. As is known to persons of ordinary skill in the art, the Xerox DataGlyph™ Technology represents digital information with machine readable data which is encoded into many, tiny, individual glyph elements. Each glyph element consists of a 45 degree diagonal line which could be as short as 1/100th of an inch depending on the resolution of the scanning and printing devices. Each glyph element represents a binary 0 or 1 depending on whether it slopes downward to the left or the right respectively. Accordingly, DataGlyph™ elements can represent character strings as ASCII or EBCIDIC binary representations. Further, encryption methods, as known to persons of ordinary skill in the art encrypt the data represented by the DataGlyph™ Technology.

The use of glyph technology in the DataTreasury™ System **100** improves the accuracy, cost and performance of the system. Xerox DataGlyph™ Technology includes error correction codes which can be referenced to correct scanning errors or to correct damage to the document caused by ink spills or ordinary wear. DataGlyph™ Technology also leads to decreased system cost since the system will require less manual intervention for data entry and correction because of the improved accuracy associated with DataGlyph elements.

Since DataGlyph elements represent a large amount of information in a small amount of space, the DAT scanner **100** will require a small amount of time to input a large amount of information.

The DAT card interface **212** and the DAT signature pad **214** along with the internet and telephone access through the DAT modem **204** enable the DataTreasury™ System **100** customer to initiate secure sale and banking transactions via the internet or telephone with the DAT **200** using a variety of cards including debit cards, smart cards and credit cards. After selecting a purchase or a banking transaction through a standard internet interface, the DataTreasury™ System **100** customer inserts or swipes the debit card, smart card or credit card into the DAT card interface **212**.

The DAT card interface **212** retrieves the identification information from the card for subsequent transmission to the destination of the internet transaction. Further, the DAT scanner **202** could capture a hand written signature from a document or the DAT signature pad **214** could capture an electronic signature written on it with a special pen. Similarly, these security features allow a credit card recipient to activate the card with a DAT **200** located at a merchant site. The security features would detect unauthorized use of debit cards, credit cards and smart cards resulting from their unlawful interception. Accordingly, the DataTreasury™ System's **100** security features offer a more secure alternative for internet and telephone transactions than the typical methods which only require transmission of a card account number and expiration date.

As is known to persons of ordinary skill in the art, the DATs **200** could also include additional devices for capturing other biometric data for additional security. These devices include facial scans, fingerprints, voice prints, iris scans, retina scans and hand geometry.

In addition to initiating sale and banking transactions, the DAT card interface **212** also reads sale and banking transactions initiated elsewhere from the memory of smart cards to enable subsequent storage and processing by the DataTreasury™ System. If a smart card is lost, stolen, damaged or deliberately altered by an unscrupulous holder after the DAT card interface **212** reads its transaction data, the DataTreasury™ System **100** can reproduce the transaction data for the customer. Accordingly, the DAT card interface **212** provides support for independent verification

of the records maintained by consumers, merchants and bankers to prevent the loss of data from the loss, theft, damage or deliberate alteration of the smart card.

The DAT card interface **212** also supports the initiation and retrieval of sale and banking transactions with the DataTreasury™ System anonymous smart cards. In contrast to standard debit cards and credit cards, the DataTreasury™ System anonymous smart card does not identify the card's holder by name. Instead, the DataTreasury™ System anonymous smart card requires only an account number and a password. Since DataTreasury™ System anonymous smart card transactions can be identified without the customer's name, a DataTreasury™ System **100** customer can purchase a DataTreasury™ System anonymous smart card, add money to the card, make expenditures with the card and monitor the card's account with the same degree of privacy as cash acquisition, expenditure and management.

The DAT scanner **202**, the internet access, the signature pad **214** and other biometric data capture devices also support the remote capture of survey information and purchase orders. For example, the DAT scanner **202** captures surveys appearing on the back of checks at restaurants and bars. Similarly, the DAT scanner **202** could capture purchase orders from residences, enabling customers to make immediate purchases from their home of goods promoted through the mail. Accordingly, home marketing merchant could transmit sales in a more cost efficient and reliable manner by using the DAT scanner **202** instead of providing envelopes with prepaid postage to residences.

The DAT scanner **202** also captures receipts which are subsequently needed for tax return preparation or tax audits. Similarly, the DAT scanner **202** captures sales receipts from merchants, providing an off-site secure, reliable repository to guard against loss resulting from flooding, fire or other circumstances. This feature could also allow a merchant to automatically perform inventory in a reliable and cost-effective manner.

The DAT controller **210** performs processing tasks and Input/Output (I/O) tasks which are typically performed by a processor. The DAT controller **210** compresses, encrypts and tags the BI to form a Tagged Encrypted Compressed Bitmap Image (TECBI). The DAT controller **210** also manages the Input/Output (I/O). Specifically, the DAT controller **210** manages devices like the DAT scanner **202**, the DAT digital storage **206**, the optional DAT printer **208** and the DAT modem **204**.

The DAT digital storage **208** holds data such as the TECBI. The DAT modem **204** transmits data from the DAT **200** to the appropriate DAC **400** as instructed by the DAT controller **210**. Specifically, the DAT modem **204** transmits the TECBIs from the DAT digital storage **208** to the appropriate DAC **400**. In the preferred embodiment, the DAT modem **204** is a high speed modem with dial-up connectivity. The DAT digital storage **208** is sufficiently large to store the input data before transmission to a DAC **400**. The DAT digital storage **208** can be Random Access Memory (RAM) or a hard drive.

FIG. **3***a* is a flow chart **300** describing the operation of the DAT in detail. In step **310**, the DAT scanner **202** scans paper receipts into the DAT **200** provided by an operator. In step **312**, the DAT controller **210** determines whether the operation executed successfully. If the scanning is successful, the DAT scanner **202** produces a Bitmap Image (BI). If the scanning is unsuccessful, the DAT controller **210** notifies the operator of the trouble and prompts the operator for repair in step **370**.

If a BI is created, the DAT controller **210** executes a conventional image compression algorithm like the Tagged Image File Format (TIFF) program to compress the BI in step **314**. In step **316**, the DAT controller **210** determines whether the compression executed successfully. If the compression is successful, it produces a Compressed Bitmap Image (CBI). If the compression is unsuccessful, the DAT controller **210** notifies the operator of the trouble and prompts the operator for repair in step **370**.

If a CBI is created, the DAT controller **210** executes an encryption algorithm which is well known to an artisan of ordinary skill in the field to encrypt the CBI in step **318**. Encryption protects against unauthorized access during the subsequent transmission of the data which will be discussed below. In step **320**, the DAT controller **210** determines whether the encryption operation executed successfully. If the encryption is successful, it produces an Encrypted Compressed Bitmap Image (ECBI). If the encryption is unsuccessful, the DAT controller **210** notifies the operator of the trouble and prompts the operator for repair in step **370**.

If an ECBI is created, the DAT controller **210** tags the ECBI with a time stamp which includes the scanning time, an identification number to identify the merchant originating the scan and any additional useful information in step **322**. In step **324**, the DAT controller **210** determines whether the tagging operation executed successfully. If the tagging is successful, it produces a Tagged Encrypted Compressed Bitmap Image (TECBI). If the tagging is unsuccessful, the DAT controller **210** notifies the operator of the trouble and prompts the operator for repair in step **370**.

If a TECBI is created, the DAT controller **210** stores the TECBI in the DAT digital storage **208** in step **326**. In step **328**, the DAT controller **210** determines whether the storing operation executed successfully. If the storing operation is successful, the DAT digital storage **208** will contain the TECBI. If the storing operation is unsuccessful, the DAT controller **210** notifies the operator of the trouble and prompts the operator for repair in step **370**.

If the TECBI is properly stored in the DAT digital storage **208**, the DAT controller **210** determines whether all paper receipts have been scanned in step **330**. If all paper receipts have not been scanned, control returns to step **310** where the next paper receipt will be processed as discussed above. If all paper receipts have been scanned, the DAT controller **210** asks the operator to verify the number of scanned receipts in step **334**. If the number of scanned receipts as determined by the DAT controller **210** does not equal the number of scanned receipts as determined by the operator, the DAT controller **210** asks whether the operator desires to rescan all of the receipts in step **338**.

If the operator chooses to rescan all of the receipts in step **338**, the DAT controller **210** will delete all of the TECBIs associated with the batch from the DAT digital storage **208** in step **342**. After the operator prepares the batch of receipts for rescan in step **346**, control returns to step **310** where the first receipt in the batch will be processed as discussed above.

If the operator chooses not to rescan all of the receipts from the batch in step **338**, control returns to step **334** where the DAT controller **210** asks the operator to verify the number of scanned receipts as discussed above.

If the number of scanned receipts as determined by the DAT controller **210** equals the number of scanned receipts as determined by the operator, the DAT controller **210** prints a batch ticket on the DAT printer **206** in step **350**. The operator will attach this batch ticket to the batch of receipts which

have been scanned. This batch ticket shall contain relevant session information such as scan time, number of receipts and an identification number for the data operator. If processing difficulties occur for a batch of receipts after the image capture of flowchart **300**, the batch ticket will enable them to be quickly located for rescanning with the DAT **200**.

In step **354**, the DAT controller **210** determines whether the scan session has completed. If the scan session has not completed, control returns to step **310** where the first receipt in the next batch of the scan session will be processed as discussed above. If the scan session has completed, the DAT controller **210** selectively prints a session report on the DAT printer **206** in step **358**. The DAT controller **210** writes statistical information for the session to the DAT digital storage **208** in step **362**. In step **366**, the DAT controller **210** terminates the session.

FIG. **3***b* displays a sample paper receipt which is processed by the DAT **200** as described by the flowchart in FIG. **3***a*. The sample paper receipt involves a credit card transaction which has four participants:

A. The ISSUER: is an entity such as a bank or corporate financial institution such as GE Capital, GM or AT&T which provides the credit behind the credit card and issues the card to the consumer.

B. The PROCESSOR: executes the processing of an inbound credit card transaction by performing basic transaction validation that includes checking with the ISSUER database to ensure that the credit card has sufficient credit to allow approval of the transaction.

C. The ACOUIRER: specializes in the marketing, installation and support of Point Of Sale (POS) credit card terminals. The acquirer, like the DAC **400** in the DataTreasury™ System **100** acts as an electronic collection point for the initial credit card transaction as the card is inserted into the POS terminal. After acquisition, the acquirer passes the transaction to the PROCESSOR.

D. The MERCHANT: inserts a credit card into a POS terminal and enters the amount of the transaction to initiate the credit card transaction.

In the preferred embodiment, the DAT **200** reads the following information from the sample paper receipt shown in FIG. **3***b* and stores the information in the format described below.

CUSTOMER_ID **370**: This field is a **7** position HEX numeric value. This field uniquely identifies the customer using the terminal. In this sample, this field would identify the credit card merchant.

TERMINAL_ID **372**: This field is a **6** position decimal numeric value. This field uniquely identifies the credit card terminal which is used to print the credit card receipt.

TRANSACTION_DATE **374**: This field contains the date and time of the credit card transaction.

TRANSACTION_LINE_ITEM **376**: This field is a variable length character string. The first three positions represent a right justified numeric field with leading zeros indicating the full length of this field. This field contains all data pertaining to the purchased item including the item's price. The DAT **200** will store a TRANSACTION_LINE_ITEM field for each transaction line item on the receipt. This field is optional since not all credit card transactions will have line items.

TRANSACTION_SUBTOTAL **378**: This field is a double precision floating point number. This field indicates the subtotal of the TRANSACTION_LINE_ITEMs.

TRANSACTION_SALES_TAX **380**: This field is a double precision floating point number. This field contains the sales tax of the TRANSACTION_SUBTOTAL.

TRANSACTION_AMOUNT **382**: This field is a double precision floating point number. This field is the sum of the TRANSACTION_SUBTOTAL and TRANSACTION_SALES_TAX.

CREDIT_CARD_ACCT_NUM **384**: This field is a **12** position decimal value. This field identifies the credit card which was used to execute this transaction.

CREDIT_CARD_EXP_DATE **386**: This field identifies the expiration date of the credit card.

TRANSACTION_APPROVAL_CODE **388**: This field is a **6** position numeric value. This field indicates the approval code that was given for the particular transaction.

The DAT **200** also stores additional items which are not pictured in FIG. **3***b* as described below:

ISSUER_ID: This field is a **7** position decimal numeric value. This field identifies the credit card issuer.

ACQUIRER_ID: This field is a **7** position decimal numeric value. This field identifies the acquirer.

PROCESSOR_ID: This field is a **7** position decimal numeric value. This field identifies the processor.

TRANSACTION_LINE_ITEM_CNT: This field is a **3** position decimal numeric value. This field identifies the number of transaction line items on the receipt. A value of ZERO indicates the absence of any transaction line items on the receipt.

TRANSACTION_GRATUITY: This field is a double precision floating number. This field is optional because it will only appear on restaurant or bar receipts.

FINAL_TRANSACTION_AMOUNT: This field is a double precision floating number. This field is optional because it will only appear on restaurant and bar receipts. The field is the sum of the TRANSACTION_AMOUNT and TRANSACTION_GRATUITY.

The tag prepended to the ECBI in step **322** of the flowchart of FIG. **3***a* identifies the time and place of the document's origination. Specifically, the tag consists of the following fields:

DAT_TERMINAL_ID: This field is a **7** position hexadecimal numeric value. This field uniquely identifies the DAT **200** which is used by the customer.

DAT_SESSION_DATE: This field identifies the date and time of the DAT **200** session which generated the image of the document.

DAT_USER_ID: This field is a 4 position decimal numeric value. This field identifies the individual within the CUSTOMER's organization who initiated the DAT **200** session.

DATA_GLYPH_RESULT: This field is a variable length character string. The first four positions hold a right justified numeric position with leading zero which indicate the length of the field. The fifth position indicates the DataGlyph™ element status. A value of 0 indicates that the data glyph was NOT PRESENT on the receipt. A value of 1 indicates that the data glyph WAS PRESENT and contained no errors. A value of 2 indicates that the data glyph WAS PRESENT and had nominal errors. If the fifth position of this field has a value of 2, the remaining portion of the string identifies the erroneous field numbers. As subsequently described, the DPC **600** will reference this portion of

the field to capture the erroneous data from the receipt with alternate methods. A value of 3 indicates that the data glyph WAS PRESENT WITH SEVERE ERRORS. In other words, a value of 3 indicates the DataGlyph™ element was badly damaged and unreadable.

The receipt shown in FIG. **3***b* can also contain a signature which can be captured by the DAT scanner **202**. A data glyph could identify the location of the signature on the receipt.

As is known to persons of ordinary skill in the art, the DataTreasury™ System **100** can also process receipts with alternate formats as long as the receipt contains the appropriate identification information such as the transaction amount, the customer, the DAT **200**, the transaction date, the transaction tax, the credit card number, the credit card expiration date, etc.

The DataTreasury™ System **100** partitions the paper receipt into image snippets as illustrated by the sample on FIG. **3***b*. Partitioning facilitates an improvement in the process to correct errors from the scanning operation. If an error occurred during scanning, the DataTreasury™ System **100** corrects the error using manual entry. With partitioning, the DataTreasury™ System **100** focuses the correction effort on only the image snippet having the error instead of correcting the entire document. The subsequently discussed schema of the DataTreasury™ System **100** database describes the implementation of the partitioning concept in detail.

The DACs **400** form the backbone of the tiered architecture shown in FIG. **1** and FIG. **4**. As shown in FIG. **1**, each DAC **400** supports a region containing a group of DATs **200**. Each DAC **400** polls the DATs **200** in its region and receives TECBIs which have accumulated in the DATs **200**. The DACs **400** are located at key central sites of maximum merchant density.

In the preferred embodiment, the DAC server **402** comprises stand-alone Digital Equipment Corporation (DEC) SMP Alpha 4100 2/566 servers which are connected on a common network running Windows NT. The DEC Alpha servers manage the collection and intermediate storage of images and data which are received from the DATs **200**.

As is known to persons of ordinary skill in the art, the DataTreasury™ System **100** could use any one of a number of different servers that are available from other computer vendors as long as the server meets the capacity, performance and reliability requirements of the system.

In the preferred embodiment, the DAC server **402** also comprises EMC **3300** SYMMETRIX CUBE Disk Storage Systems, which store the images and data collected and managed by the DEC Alpha servers. The DAC **400** architecture also uses a SYMMETRIX Remote Data Facility (SRDF), available from EMC, to enable multiple, physically separate data centers housing EMC Storage Systems to maintain redundant backups of each other across a Wide Area Network (WAN). Since SRDF performs the backup operations in the background, it does not affect the operational performance of the DataTreasury™ System **100**. The DAC server **402** also has secondary memory **410**. In the preferred embodiment, the secondary memory **410** is a small scale DLT jukebox.

The DAC Alpha servers of the DAC server **402** insert images and data received from the DATs **200** into a database which is stored on the disk storage systems using a data manipulation language as is well known to persons of ordinary skill in the art. In the preferred embodiment, the database is a relational database available from Oracle.

As is well known to persons of ordinary skill in the art, the DataTreasury™ System **100** could use any one of a number of different database models which are available from other vendors including the entity relationship model as long as the selected database meets the storage and access efficiency requirements of the system. See, e.g., Chapter 2 of Database System Concepts by Korth and Silberschatz.

The DAC **400** architecture uses a WEB based paradigm using an enhanced Domain Name Services (DNS), the Microsoft Component Object Model (DCOM), and Windows NT Application Program Interfaces (APIs) to facilitate communication and load balancing among the servers comprising the DAC server **402**. As is known to persons of ordinary skill in the art, DNS, which is also known as Bind, statically translates name requests to Internet Protocol 4 (IP4) addresses. In the DAC **400** architecture, an enhanced DNS dynamically assigns IP4 addresses to balance the load among the servers comprising the DAC server **402**.

In the preferred embodiment, the enhanced DNS is designed and implemented using objects from Microsoft DCOM. Using the DCOM objects, the enhanced DNS acquires real-time server load performance statistics on each server comprising the DAC server **402** from the Windows NT API at set intervals. Based on these load performance statistics, the enhanced DNS adjusts the mapping of name requests to IP4 addresses to direct data toward the servers which are more lightly loaded.

A large bank of modems **404** polls the DATs **200** at the customer sites within the DAC's **400** region. In the preferred embodiment, the bank of modems **404**, available as CISCO AS5200, is an aggregate **48** modem device with Local Area Network (LAN) **406** connectivity which permits the DAC servers **402** to dial the DATs **200** without requiring 48 separate modems and serial connections.

The DAC servers **402** and the bank of modems **404** are connected on a LAN **406**. In the preferred embodiment, the LAN uses a switched 100BaseT/10BaseT communication hardware layer protocol. As is known to persons of ordinary skill in the art, the 100BaseT/10BaseT protocol is based on the Ethernet model. Further, the numbers 100 and 10 refer to the communication link speed in megabits per second. In the preferred embodiment, the CISCO Catalyst 2900 Network Switch supports the LAN **406** connectivity between the devices connected to the LAN **406** including the DAC servers **402** and the bank of modems **404**.

As is known to persons of ordinary skill in the art, alternate LAN architectures could be used to facilitate communication among the devices of the LAN **406**. For example, the LAN **406** could use a hub architecture with a round robin allocation algorithm, a time division multiplexing algorithm or a statistical multiplexing algorithm.

A Wide Area Network (WAN) router **408** connects the LAN **406** to the WAN to facilitate communication between the DACs **400** and the DPCs **600**. In the preferred embodiment, the WAN router **408** is a CISCO 4700 WAN Router. The WAN router **408** uses frame relay connectivity to connect the DAC LAN **406** to the WAN. As is known to persons of ordinary skill in the art, alternate devices, such as the NORTEL Magellen Passport "50" Telecommunication Switch, could be used to facilitate communication between the DACs **400** and the DPCs **600** as long as the selected router meets the performance and quality communication requirements of the system.

As is known to persons of ordinary skill in the art, frame relay is an interface protocol for statistically multiplexed packet-switched data communications in which variable-sized packets (frames) are used that completely enclose the user packets which they transport. In contrast to dedicated point to point links that guarantee a specific data rate, frame

relay communication provides bandwidth on-demand with a guaranteed minimum data rate. Frame relay communication also allows occasional short high data rate bursts according to network availability.

Each frame encloses one user packet and adds addressing and verification information. Frame relay data communication typically has transmission rates between 56 kilobytes per second (kb/s) and 1.544 megabytes per second (Mb/s). Frames may vary in length up to a design limit of approximately 1 kilobyte.

The Telco Carrier Cloud **412** is a communication network which receives the frames destined for the DPC **600** sent by the WAN router **408** from the DACs **400**. As is known to persons of ordinary skill in the art, carriers provide communication services at local central offices. These central offices contain networking facilities and equipment to interconnect telephone and data communications to other central offices within its own network and within networks of other carriers.

Since carriers share the component links of the interconnection network, data communication must be dynamically assigned to links in the network according to availability. Because of the dynamic nature of the data routing, the interconnection network is referred to as a carrier cloud of communication bandwidth.

All the DAC **400** equipment is on fully redundant on-line UPS power supplies to insure maximum power availability. Further, to minimize the time for trouble detection, trouble analysis and repair, all the DAC **400** equipment incorporates trouble detection and remote reporting/diagnostics as is known to an artisan of ordinary skill in the art.

FIG. **5** is a flow chart **500** describing the polling of the DATs **200** by a DAC **400** and the transmission of the TECBIs from the DATs **200** to the DAC **400**. In step **502**, the DAC server **402** reads the address of the first DAT **200** in its region for polling. In step **504**, a modem in the modem bank **404** dials the first DAT **200**. The DAC **400** determines whether the call to the DAT **200** was successful in step **506**. If the call to the first DAT **200** was unsuccessful, the DAC **400** will record the error condition in the session summary report and will report the error to the DPC **600** in step **522**.

If the call to the first DAT **200** was successful, the DAC **400** will verify that the DAT **200** is ready to transmit in step **508**. If the DAT **200** is not ready to transmit, the DAC **400** will record the error condition in the session summary report and will report the error to the DPC **600** in step **522**.

If the DAT **200** is ready to transmit in step **508**, the DAT **200** will transmit a TECBI packet header to the DAC **400** in step **510**. The DAC **400** will determine whether the transmission of the TECBI packet header was successful in step **512**. If the transmission of the TECBI packet header was unsuccessful, the DAC **400** will record the error condition in the session summary report and will report the error to the DPC **600** in step **522**.

If the transmission of the TECBI packet header was successful in step **512**, the DAT **200** will transmit a TECBI packet to the DAC **400** in step **514**. The DAC **400** will determine whether the transmission of the TECBI packet was successful in step **516**. If the transmission of the TECBI packet header was unsuccessful, the DAC **400** will record the error condition in the session summary report and will report the error to the DPC **600** in step **522**.

If the transmission of the TECBI packet was successful in step **516**, the DAC **400**, in step **518**, will compare the TECBI packet header transmitted in step **510** to the TECBI packet transmitted in step **514**. If the TECBI packet header does not match the TECBI packet, the DAC **400** will record the error condition in the session summary report and will report the error to the DPC **600** in step **522**.

If the TECBI packet header matched the TECBI packet in step **518**, the DAC **400** will set the status of the TECBI packet to indicate that it is ready for transmission to the DPC **600** in step **520**. The DAC **400** will also transmit the status to the DAT **200** to indicate successful completion of the polling and transmission session in step **520**. Next, the DAC **400** will determine whether TECBIs have been transmitted from all of the DATs **200** in its region in step **524**. If all DATs **200** in the DAC's **400** region have transmitted TECBIs to the DAC **400**, the DAC **400** will compile a DAT **200** status report in step **528** before terminating the session.

If one or more DATs **200** in the DAC's **400** region have not transmitted TECBIs to the DAC **400**, the DAC **400** will get the address of the next DAT **200** in the region in step **526**. Next, control returns to step **504** where the next DAT **200** in the DAC's **400** region will be polled as previously discussed.

In the preferred embodiment, the DAC server **402** initiates the polling and data transmission at optimum toll rate times to decrease the cost of data transmission. In addition to the raid drives and redundant servers, the DAC **400** will also have dual tape backup units which will periodically backup the entire data set. If there is a catastrophic failure of the DAC **400**, the tapes can be retrieved and sent directly to the DPC **600** for processing. As the DAT **200** polling and data transmission progresses, the DAC **400** will periodically update the DPC **600** with its status. If there is a catastrophic failure with the DAC **400**, the DPC **600** would know how much polling and backup has been done by the failing DAC **400**. Accordingly, the DPC **600** can easily assign another DAC **400** to complete the polling and data transmission for the DATs **200** in the failed DAC's **400** region.

FIG. **6** is a block diagram of the DPC **600** architecture. The DPC **600** accumulates, processes and stores images for later retrieval by DataTreasury™ System retrieval customers who have authorization to access relevant information. DataTreasury™ System retrieval customers include credit card merchants, credit card companies, credit information companies and consumers. As shown in FIG. **6** and FIG. **1**, the DPC **600** polls the DACs **400** and receives TECBIs which have accumulated in the DACs **400**.

In the preferred embodiment, the DPC server **602** comprises stand-alone Digital Equipment Corporation (DEC) SMP Alpha 4100 4/566 servers which are connected on a common network running Windows NT. The DEC Alpha servers manage the collection and intermediate storage of images and data which are received from the DACs **400**.

In the preferred embodiment, the DPC server **602** also comprises EMC 3700 SYMMETRIX CUBE Disk Storage Systems, which store the images and data collected and managed by the DEC Alpha servers. Like the DAC **400** architecture, the DPC **600** architecture uses a SYMMETRIX Remote Data Facility (SRDF), available from EMC, to enable multiple, physically separate data centers housing EMC Storage Systems to maintain redundant backups of each other across a Wide Area Network (WAN).

Like the DAC **400** architecture, the DPC **600** architecture uses a WEB based paradigm using an enhanced Domain Name Services (DNS), the Microsoft Component Object Model (DCOM), and Windows NT Application Program Interfaces (APIs) to facilitate communication and load balancing among the servers comprising the DPC server **602** as described above in the discussion of the DAC **400** architecture.

The workstation **604** performs operation control and system monitoring and management of the DPC **600** net-

work. In the preferred embodiment, the workstation **604**, available from Compaq, is an Intel platform workstation running Microsoft Windows NT 4.x. The workstation **604** should be able to run Microsoft Windows NT 5.x when it becomes available. The workstation **604** executes CA Unicenter TNG software to perform network system monitoring and management. The workstation **604** executes SnoBound Imaging software to display and process TECBIs.

The workstation **604** also performs identification verification by comparing signature data retrieved remotely by the DATs **200** with signature data stored at the DPC **600**. In the preferred embodiment, signature verification software, available from Communications Intelligence Corporation of Redwood Shores, Calif. executing on the workstation **604** performs the identification verification. As is known to persons of ordinary skill in the art, the workstation **604** could execute other software to perform identification verification by comparing biometric data including facial scans, fingerprints, retina scans, iris scans and hand geometry. Thus, the DPC **600** could verify the identity of a person who is making a purchase with a credit card by comparing the biometric data captured remotely with the biometric data stored at the DPC **600**.

As is known to persons of ordinary skill in the art, the DataTreasury™ System **100** could use workstations with central processing units from other integrated circuit vendors as long as the chosen workstation has the ability to perform standard operations such as fetching instructions, fetching data, executing the fetched instructions with the fetched data and storing results. Similarly, the DataTreasury™ System **100** could use alternate windows operating systems and network monitoring software as long as the selected software can monitor the status of the workstations and links in the network and display the determined status to the operator. The Remote Data Entry Gateway **614** and the Remote Offsite Data Entry Facilities **616** correct errors which occurred during data capture by the DAT **200**. Since the DataTreasury™ System **100** partitions the document as described in the discussion of the sample receipt of FIG. **3***b*, the operator at the Remote Data Entry Gateway **614** or the Remote Offsite Date Entry Facilities **616** only needs to correct the portion of the document or image snippet which contained the error.

Partitioning improves system performance, decreases system cost and improves system quality. With partitioning, the DPC Server **602** only sends the portion of the document containing the error to the Remote Data Entry Gateway **614** or the Remote Offsite Data Entry Facilities **616**. Since the operator at these data entry locations only sees the portion of the document which contained the error, she can quickly recognize and correct the error. Without partitioning, the operator would have to search for the error in the entire document. With this inefficient process, the operator would need more time and would be more likely to make a mistake by missing the error or making a modification in the wrong location. Accordingly, partitioning improves system performance and quality by increasing the speed and accuracy of the error correction process.

Similarly, partitioning decreases the traffic on the DPC LAN **606** and the Telco Carrier Cloud **412** because the DPC Server **602** only sends the image snippet containing the error to the Remote Offsite Data Entry Facility **616** or the Remote Data Entry Gateway **614**. Accordingly, partitioning decreases system cost by reducing the bandwidth requirement on the interconnection networks.

A DPC LAN **606** facilitates communication among the devices which are connected to the LAN **606** including the DPC server **602** and the network workstation **604**. In the preferred embodiment, the DPC LAN **606** uses a switched 100BaseT/10BaseT communication hardware layer protocol like the DAC LAN **406** discussed earlier. In the preferred embodiment, the DPC LAN **406** is a high speed OC2 network topology backbone supporting TCP/IP. The CISCO Catalyst 5500 Network Switch supports the DPC LAN **606** connectivity among the devices connected to the LAN **606**.

As is known to persons of ordinary skill in the art, alternate LAN architectures could be used to facilitate communication among the devices of the LAN **406**. For example, the LAN **406** could use a hub architecture with a round robin allocation algorithm, a time division multiplexing algorithm or a statistical multiplexing algorithm.

A Wide Area Network (WAN) router **612** connects the DPC LAN **606** to the WAN to facilitate communication between the DACs **400** and the DPCs **600**. In the preferred embodiment, the WAN router **612** is a CISCO 7507 WAN Router. The WAN router **612** uses frame relay connectivity to connect the DPC LAN **612** to the WAN. As is known to persons of ordinary skill in the art, alternate devices, such as the NORTEL Magellen Passport "50" Telecommunication Switch, could be used to facilitate communication between the DACs **400** and the DPCs **600** as long as the selected router meets the performance and quality communication requirements of the system.

The DPC **600** has a three tier storage architecture to support the massive storage requirement on the DataTreasury™ System **100**. In the preferred embodiment, the storage architecture consists of Fiber Channel RAID technology based EMC Symmetrix Enterprise Storage Systems where individual cabinets support over 1 Terabyte of storage. After TECBI images have been processed and have been on-line for 30 days, they will be moved to DVD based jukebox systems. After the TECBI images have been on-line for 90 days, they will be moved to Write Once Read Many (WORM) based jukebox systems **608** for longer term storage of up to 3 years in accordance with customer requirements.

In an alternate embodiment, the DPC **600** is intended to also configure a High Density Read Only Memory (HD-ROM) when it becomes available from NORSAM Technologies, Los Alamos, N. Mex., into optical storage jukebox systems **610**, such as that which is available from Hewlett Packard, to replace the DVD components for increased storage capacity. The HD-ROM conforms to CD-ROM form factor metallic WORM disc. The HD-ROM currently has a very large storage capacity of over 320 giga bytes (320 GB) on a single platter and has an anticipated capacity of several terabytes (TB) on a single platter. The DPC **600** uses IBM and Philips technology to read from the HD-ROM and to write to the HD-ROM.

The DPC Alpha servers of the DPC server **602** insert images and data received from the DACs **400** into a single database which is stored on the Digital Storage Works Systems using a data manipulation language as is well known to persons of ordinary skill in the art. In the preferred embodiment, the database is the V8.0 Oracle relational database which was designed to support both data and image storage within a single repository.

As known to persons of ordinary skill in the art, a relational database consists of a collection of tables which have a unique name. See, e.g., Chapter Three of Database System Concepts by Korth and Silberschatz. A database schema is the logical design of the database. Each table in a relational database has attributes. A row in a table represents a relationship among a set of values for the attributes

in the table. Each table has one or more superkeys. A superkey is a set of one or more attributes which uniquely identify a row in the table. A candidate key is a superkey for which no proper subset is also a superkey. A primary key is a candidate key selected by the database designer as the means to identify a row in a table.

As is well known to persons of ordinary skill in the art, the DataTreasury™ System **100** could use other database models available from other vendors including the entity relationship model as long as the selected database meets the storage and access efficiency requirements of the system. See, e.g., Chapter 2 of Database System Concepts by Korth and Silberschatz.

An exemplary DPC **600** basic schema consists of the tables listed below. Since the names of the attributes are descriptive, they adequately define the attributes' contents. The primary keys in each table are identified with two asterisks (**). Numeric attributes which are unique for a particular value of a primary key are denoted with the suffix, "NO". Numeric attributes which are unique within the entire relational database are denoted with the suffix, "NUM".

I. CUSTOMER: This table describes the DataTreasury ™ System customer.
- A. **CUSTOMER_ID
- B. COMPANY_NAME
- C. CONTACT
- D. CONTACT_TITLE
- E. ADDR1
- F. ADDR2
- G. CITY
- H. STATE_CODE
- I. ZIP_CODE
- J. COUNTRY_CODE
- K. VOX_PHONE
- L. FAX_PHONE
- M. CREATE_DATE

II. CUSTOMER_MAIL_TO: This table describes the mailing address of the DataTreasury ™ System customer.
- A. **MAIL_TO_NO
- B. **CUST_ID
- C. CUSTOMER_NAME
- D. CONTACT
- E. CONTACT_TILE
- F. ADDR1
- G. ADDR2
- H. CITY
- I. STATE_CODE
- J. ZIP_CODE
- K. COUNTRY_CODE
- L. VOX_PHONE
- M. FAX_PHONE
- N. CREATE_DATE
- O. COMMENTS

III. CUSTOMER_DAT_SITE: This table describes the DAT location of the DataTreasury ™ System customer.
- A. **DAT_SITE_NO
- B. **CUST_ID
- C. CUSTOMER_NAME
- D. CONTACT
- E. CONTACT_TILE
- F. ADDR1
- G. ADDR2
- H. CITY
- I. STATE_CODE
- J. ZIP_CODE
- K. COUNTRY_CODE
- L. VOX_PHONE
- M. FAX_PHONE
- N. CREATE_DATE
- O. COMMENTS

-continued

IV. CUSTOMER_SITE_DAT: This table describes the DAT site(s) of the DataTreasury ™ System customer.
- A. **DAT_TERMINAL_ID
- B. **DAT_SITE_NO
- C. **CUST_ID
- D. INSTALL_DATE
- E. LAST_SERVICE_DATE
- F. CREATE_DATE
- G. COMMENTS

V. DATA_SPEC: This table provides data specifications for document partitioning and extraction.
- A. **DATA_SPEC_ID
- B. **CUST_ID
- C. DESCR
- D. RECORD_LAYOUT_RULES
- E. CREATE_DATE
- F. COMMENTS

VI. DATA_SPEC_FIELD: This table provides field data specifications for document partitioning and extraction.
- A. **DATA_SPEC_NO
- B. **DATA_SPEC_ID
- C. FIELD_NAME
- D. DESCR
- E. DATA_TYPE
- F. VALUE_MAX
- G. VALUE_MIN
- H. START_POS
- I. END_POS
- J. FIELD_LENGTH
- K. RULES
- L. CREATE_DATE
- M. COMMENTS

VII. TEMPL_DOC: This table specifies the partitioning of a predefined document.
- A. **TEMPL_DOC_NUM
- B. DATA_SPEC_ID
- C. DESCR
- D. RULES
- E. CREATE_DATE
- F. COMMENTS

VIII. TEMPL_FORM: This table defines the location of forms on a predefined document.
- A. **TEMPL_FORM_NO
- B. **TEMPL_DOC_NUM
- C. SIDES_PER_FORM
- D. MASTER_IMAGE_SIDE_A
- E. MASTER_IMAGE_SIDE_B
- F. DISPLAY_ROTATION_A
- G. DISPLAY_ROTATION_B
- H. DESCR
- I. RULES
- J. CREATE_DATE

IX. TEMPL_PANEL: This table specifies the location of panels within the forms of a predefined document.
- A. **TEMPL_PANEL_NO
- B. **TEMPL_SIDE_NO
- C. **TEMPL_FORM_NO
- D. **TEMPL_DOC_NUM
- E. DISPLAY_ROTATION
- F. PANEL_UL_X
- G. PANEL_UL_Y
- H. PANEL_LR_X
- I. PANEL_LR_Y
- J. DESCR
- K. RULES
- L. CREATE_DATE

X. TEMPL_FIELD: Thls table defines the location of fields within the panels of a form of a predefined document.
- A. **TEMPL_FIELD_NO
- B. **TEMPL_PANEL_NO
- C. **TEMPL_SIDE_NO
- D. **TEMPL_FORM_NO
- E. **TEMPL_DOC_NUM
- F. DISPLAY_ROTATION
- G. FLD_UL_X

-continued

	H.	FLD_UL_Y
	I.	FLD_LR_X
	J.	FLD_LR_Y
	K.	DESCR
	L.	RULES
	M.	CREATE_DATE
XI.	DAT_BATCH: This table defines batches of documents which were processed during a DAT session.	
	A.	**DAT_BATCH_NO
	B.	**DAT_SESSION_NO
	C.	**DAT_SESSION_DATE
	D.	**DAT_TERMINAL_ID
	E.	DAT_UNIT_CNT
	F.	CREATE_DATE
XII.	DAT_UNIT: This table defines the unit in a batch of documents which were processed in a DAT session.	
	A.	**DAT_UNIT_NUM
	B.	**DAT_BATCH_NO
	C.	**DAT_SESSION_NO
	D.	**DAT_SESSION_DATE
	E.	**DAT_TERMINAL_ID
	F.	FORM_CNT
	G.	DOC_CNT
	H.	CREATE_DATE
XIII.	DAT_DOC: This table defines documents in the unit of documents which were processed in a DAT session.	
	A.	**DAT_DOC_NO
	B.	**DAT_UNIT_NUM
	C.	DOC_RECORD_DATA
	D.	CREATE_DATE

The DATA_SPEC, DATA_SPEC_FIELD, TEMPL_DOC, TEMPL_FORM, TEMPL_PANEL and TEMPL_FIELD tables implement the document partitioning algorithm mentioned above in the discussion of the sample receipt of FIG. **3***b*. The cross product of the DATA_SPEC and DATA_SPEC_FIELD tables partition arbitrary documents while the cross product of the TEMPL_DOC, TEMPL_FORM, TEMPL_PANEL and TEMPL_FIELD tables partition predefined documents of the DataTreasury™ System **100**. The TEMPL_FORM defines the location of forms on a predefined document. The TEMPL_PANEL defines the location of panels within the forms of a predefined document. Finally, the TEMPL_FIELD table defines the location of fields within the panels of a form of a predefined document.

The DPC **600** performs data mining and report generation for a wide variety of applications by returning information from the data base. For example, the DPC **600** generates market trend analysis reports and inventory reports for merchants by analyzing the data from receipts captured by the DAT **200**. The DPC **600** also can provide important tax information to the taxpayer in the form of a report or to software applications like tax preparation software by retrieving tax information from the database which originally resided on receipts, documents and electronic transactions captured by the DAT **200**. Similarly, the DPC **600** can also provide tax information for particular periods of time for a tax audit.

FIG. **7** is a flow chart **700** describing the polling of the DACs **300** by a DPC **600** and the transmission of the TECBIs from the DACs **300** to the DPC **600**. In step **702**, the DPC **600** reads the address of the first DAC **300** in its region for polling.

In step **704**, the DPC **600** connects with a DAC **300** for transmission. The DPC **600** determines whether the connection to the DAC **300** was successful in step **706**. If the call to the DAC **300** was unsuccessful, the DPC **600** will record the error condition in the session summary report and will report the error to the DPC **600** manager in step **722**.

If the connection to the DAC **300** was successful, the DPC **600** will verify that the DAC **300** is ready to transmit in step **708**. If the DAC **300** is not ready to transmit, the DPC **600** will record the error condition in the session summary report and will report the error to the DPC **600** manager in step **722**.

If the DAC **300** is ready to transmit in step **708**, the DAC **300** will transmit a TECBI packet header to the DPC **600** in step **710**. The DPC **600** will determine whether the transmission of the TECBI packet header was successful in step **712**. If the transmission of the TECBI packet header was unsuccessful, the DPC **600** will record the error condition in the session summary report and will report the error to the DPC **600** manager in step **722**.

If the transmission of the TECBI packet header was successful in step **712**, the DAC **300** will transmit a TECBI packet to the DPC **600** in step **714**. The DPC **600** will determine whether the transmission of the TECBI packet was successful in step **716**. If the transmission of the TECBI packet header was unsuccessful, the DPC **600** will record the error condition in the session summary report and will report the error to the DPC **600** manager in step **722**.

If the transmission of the TECBI packet was successful in step **716**, the DPC **600**, in step **718**, will compare the TECBI packet header transmitted in step **710** to the TECBI packet transmitted in step **714**. If the TECBI packet header does not match the TECBI packet, the DPC **600** will record the error condition in the session summary report and will report the error to the DPC **600** manager in step **722**.

If the TECBI packet header matched the TECBI packet in step **718**, the DPC **600** will set the status of the TECBI packet to indicate that it was received at the DPC **600** in step **720**. The DPC **600** will also transmit the status to the DAC **300** to indicate successful completion of the polling and transmission session in step **720**. Next, the DPC **600** will determine whether TECBIs have been transmitted from all of the DACs **300** in its region in step **724**. If all DACs **300** in the DPC's **600** region have transmitted TECBIs to the DPC **600**, the DPC **600** will compile a DAC **300** status report in step **728** before terminating the session.

If one or more DACs **300** in the DPC's **600** region have not transmitted TECBIs to the DPC **600**, the DPC **600** will get the address of the next DAC **300** in the region in step **726**. Next, control returns to step **704** where the next DAC **300** in the DPC's **600** region will be polled as previously discussed.

FIG. **8** is a flow chart **800** describing the data processing performed by the DPC **600**. In step **802**, the DPC **600** fetches the first TECBI packet. Next, the DPC **600** extracts the first TECBI from the TECBI packet in step **804**. In step **806**, the DPC **600** inserts the TECBI into the database. In step **808**, the DPC **600** extracts the tag header which includes the customer identifier, the encryption keys and the template identifier from the TECBI to obtain the ECBI.

In step **810**, the DPC **600** decrypts the ECBI image to obtain the CBI. In step **812**, the DPC **600** uncompresses the CBI to obtain the BI. In step **814**, the DPC **600** fetches and applies the BI template against the BI. Further the DPC **600** divides the BI into image snippets and tags the BI template with data capture rules in step **814** to form the Tagged Bitmap Image Snippets (TBIS). In step **816**, the DPC **600** submits the TBISs for data capture operations to form the IS Derived Data Record (ISDATA). The DPC **600** discards the TBISs upon completion of the data capture operations in step **816**. In step **818**, the DPC **600** updates the TECBI record in the database with the IS Derived Data.

In step **820**, the DPC **600** determines whether it has processed the last TECBI in the TECBI packet. If the last TECBI in the TECBI packet has not been processed, the DPC **600** extracts the next TECBI from the TECBI packet in step **822**. Next, control returns to step **806** where the next TECBI will be processed as described above.

If the last TECBI in the TECBI packet has been processed, the DPC **600** determines whether the last TECBI packet has been processed in step **824**. If the last TECBI packet has not been processed, the DPC **600** fetches the next TECBI packet in step **826**. Next, control returns to step **804** where the next TECBI packet will be processed as described above. If the last TECBI packet has been processed in step **824**, the DPC **600** terminates data processing.

As is known to persons of ordinary skill in the art, a user can request information from a relational database using a query language. See, e.g., Chapter Three of Database System Concepts by Korth and Silberschatz. For example, a user can retrieve all rows of a database table having a primary key with particular values by specifying the desired primary key's values and the table name on a select operation. Similarly, a user can retrieve all rows from multiple database tables having primary keys with particular values by specifying the desired primary keys' values and the tables with a select operation.

The DataTreasury™ System provides a simplified interface to its retrieval customers to enable data extraction from its relational database as described in FIG. **9**. For example, a DataTreasury™ System customer can retrieve the time, date, location and amount of a specified transaction.

The DPC **600** performs data mining and report generation for a wide variety of applications by returning information from the data base. For example, the DPC **600** generates market trend analysis reports and inventory reports for merchants by analyzing the data from receipts captured by the DAT **200**. The DPC **600** also can provide important tax information to the taxpayer in the form of a report or to tax preparation software by retrieving tax information from the database which originally resided on receipts, documents and electronic transactions captured by the DAT **200**. Similarly, the DPC **600** can also provide tax information for particular periods of time for a tax audit.

FIG. **9** is a flowchart **900** describing the data retrieval performed by the DPC **600**. In step **902**, the DPC **600** receives a TECBI retrieval request. In step **904**, the DPC **600** obtains the customer identifier. In step **906**, the DPC **600** determines whether the customer identifier is valid. If the customer identifier is not valid, control returns to step **904** where the DPC **600** will obtain another customer identifier.

If the customer identifier is valid in step **906**, the DPC **600** will obtain the customer security profile in step **908**. In step **910**, the DPC **600** receives a customer retrieval request. In step **912**, the DPC **600** determines whether the customer retrieval request is consistent with the customer security profile. If the customer retrieval request is not consistent with the customer security profile, control returns to step **910** where the DPC **600** will obtain another customer retrieval request. If the customer retrieval request is consistent with the customer security profile, the DPC **600** will transmit the results to the customer as indicated by the customer security profile in step **914**.

FIG. **10** is a flow chart describing the use of the DataTreasury™ system to process checks. In step **1004**, the DataTreasury™ system captures the check at the payer's remote location in the preferred embodiment before the payer presents the check to the payee. Alternatively, the payer simply presents or mails the check to the payee. The capture of the check at the payer's remote location in step **1004** enables subsequent comparison of the check as written by the payer with the check as received by the payee. In other words, this step enables the detection of check alteration from fraudulent check schemes where a check is intercepted before receipt by the payee and chemically washed to allow the perpetrator to work with a blank check.

In step **1006**, the DataTreasury™ system captures the check and the payer's biometric data at the payee's remote location. In an alternate embodiment, the DataTreasury™ system sends electronic transaction data representing the check from the payer's remote location to the payer's remote location. In step **1008**, the DataTreasury™ system performs verification of the check and biometric data by comparing the remotely captured data with the data stored at a central location. The validation further includes checking the courtesy amount and the payer's signature.

In step **1010**, the DataTreasury™ system determines whether the verification was successful. If the verification of step **1010** was not successful, the system transmits an error message to the remote locations in step **1012** and returns to step **1004** for resubmission. If the verification of step **1010** was successful, the system creates an electronic transaction representing the check at a central location in step **1014**. The electronic transaction representing the check consists of the payer bank's identification number, routing information, the payer's account number, a payer's check, a payer bank's draft, the amount of the check or draft, the payee bank's identification number, the payee bank's routing information, and the payee's account number. In step **1016**, the electronic transaction representing the check is transmitted to the payee bank. In step **1018**, the payee bank transmits the electronic transaction representing the check to the payer bank.

In step **1020**, the payer bank verifies the electronic transaction representing the check and determines whether to approve a fund transfer. If the payee bank grants approval in step **1020**, the payer bank transfers the funds from the payer bank to the payee bank in step **1022**. In step **1024**, the DataTreasury™ system notifies the payee bank and the remote locations as to the status of the transfer.

While the above invention has been described with reference to certain preferred embodiments, the scope of the present invention is not limited to these embodiments. One skilled in the art may find variations of these preferred embodiments which, nevertheless, fall within the spirit of the present invention, whose scope is defined by the claims set forth below.

What is claimed is:

1. A system for central management, storage and report generation of remotely captured paper transactions from checks comprising:

one or more remote data access subsystems for capturing and sending paper transaction data including a payer bank's routing number, a payer bank's routing information, a payer's account number, a payer's check, a payer bank's draft, a check amount, a payee bank's identification number, a payee bank's routing information, and a payee's account number, and further including subsystem identification information comprising at least one imaging subsystem for capturing the checks and at least one data access controller for managing the capturing and sending of the transaction data;

at least one central data processing subsystem for processing, sending, verifying and storing the paper transaction data and the subsystem identification information comprising a data management subsystem for

managing the processing, sending and storing of the transaction data; and

at least one communication network for the transmission of the transaction data within and between said one or more data access subsystems and said at least one data processing subsystem, with the data access subsystem providing encrypted subsystem identification information and encrypted paper transaction data to the data processing subsystem.

2. A system as in claim **1** wherein said one or more data access subsystems further comprise at least one scanner for capturing the paper transaction data.

3. A system as in claim **2** wherein said one or more data access subsystems also capture electronic transactions from credit cards, smart cards and debit cards, signature data or biometric data, further comprising:

at least one card interface for capturing the electronic transaction data;

at least one signature interface for capturing an electronic signature; and

at least one biometric interface for capturing biometric data.

4. A system as in claim **3** wherein said at least one data access controller successively transforms the captured transaction data to a bitmap image, a compressed bitmap image, an encrypted, compressed bitmap image and an encrypted, compressed bitmap image tagged with information identifying a location and time of the transaction data capture.

5. A system as in claim **4** wherein said one or more data access subsystems further comprise digital storage for storing the tagged, encrypted, compressed bitmap image.

6. A system as in claim **5** wherein said at least one card interface initiates the electronic transaction.

7. A system as in claim **6** wherein said one or more data access subsystems further comprise at least one printer for printing the paper transaction initiated by said at least one card interface.

8. A system as in claim **7** wherein the paper transaction printed by said at least one printer includes data glyphs.

9. A system as in claim **1** wherein said data management subsystem of said at least one data processing subsystem comprises:

at least one server for polling said one or more remote data access subsystems for transaction data;

a database subsystem for storing the transaction data in a useful form;

a report generator for generating reports from the transaction data and providing data to software applications;

at least one central processing unit for managing the storing of the transaction data;

a domain name services program for dynamically assigning one of said at least one server to receive portions of the transaction data for balancing the transaction data among said at least one server; and

a memory hierarchy.

10. A system as in claim **9** wherein said at least one server also polls for biometric and signature data, said database stores the biometric data and the signature data, and said at least one central processing unit verifies the biometric data and the signature data.

11. A system as in claim **9** wherein said memory hierarchy comprises at least one primary memory for storage of recently accessed transaction data and at least one secondary memory for storage of other transaction data.

12. A system as in claim **11** wherein said at least one secondary memory comprises at least one write once read many jukebox and at least one optical storage jukebox.

13. A system as in claim **12** wherein said at least one optical storage jukebox comprises read only memory technology including compact disc read only memory form factor metallic write once read many disc.

14. A system as in claim **9** wherein said database subsystem comprises at least one predefined template for partitioning the stored transaction data into panels and identifying locations of the panels.

15. A system as in claim **14** wherein said data processing subsystem further comprises a data entry gateway for correcting errors in the panels of stored transaction data.

16. A system as in claim **1** wherein said at least one communication network comprises:

at least one first local area network for transmitting data within a corresponding one of said one or more remote data access subsystems;

at least one second local area network for transmitting data within a corresponding one of said at least one data processing subsystem; and

at least one wide area network for transmitting data between said one or more remote data access subsystems and said at least one data processing subsystem.

17. A system as in claim **16** wherein said at least one communication network further comprises:

at least one modem for connecting said at least one first local area network of said one or more data access subsystems to a corresponding one of said at least one second local area network of said at least one data processing subsystem through said at least one wide area network; and

at least one bank of modems for connecting said at least one second local area network of said at least one data processing subsystem to a corresponding some of said at least one first local area network of said one or more data access subsystems through said at least one wide area network.

18. A system as in claim **1** further comprising at least one data collecting subsystem for collecting and sending the electronic or paper transaction data comprising a further management subsystem for managing the collecting and sending of the transaction data.

19. A system as in claim **18** wherein said further data management subsystem of said at least one data collecting subsystem comprises:

at least one server for polling said one or more remote data access subsystems for transaction data;

a database for storing the transaction data in a useful form;

at least one central processing unit for managing the collecting of the transaction data;

a domain name services program for dynamically assigning one of said at least one server to receive portions of the transaction data for balancing the transaction data among said at least one server; and

a memory hierarchy.

20. A system as in claim **19** wherein said memory hierarchy comprises at least one primary memory for collecting transaction data and at least one secondary memory for backup storage of the transaction data.

21. A system as in claim **20** wherein said at least one secondary memory comprises at least one DLT jukebox.

22. A system as in claim **18** wherein said at least one communication network comprises:

at least one first local area network for transmitting data within a corresponding one of said one or more remote data access subsystems;

at least one second local area network for transmitting data within a corresponding one of said at least one data collection subsystem;

at least one third local area network for transmitting data within a corresponding one of said at least one data processing subsystem; and

at least one wide area network for transmitting data between said one or more remote data access subsystems, said at least one data collection subsystem and said at least one data processing subsystem.

23. A system as in claim **22** wherein said at least one communication network further comprises:

at least one first modem for connecting said at least one first local area network of said one or more data access subsystems to a corresponding one of said at least one second local area network through said at least one wide area network;

at least one bank of modems for connecting said at least one second local area network of said at least one data collection subsystem to a corresponding some of said at least one first local area network of said one or more data access subsystems through said at least one wide area network;

at least one first wide area network router for connecting a corresponding one of said at least one second local area network of said at least one data collecting subsystem to said at least one wide area network; and

at least one second wide area network router for connecting a corresponding one of said at least one third local area network of said at least one data processing subsystem to said at least one wide area network.

24. A system as in claim **23** wherein said at least one first wide area network and said at least one second wide area network comprises a carrier cloud, said carrier cloud using a frame relay method for transmitting the transaction data.

25. A system as in claim **22** wherein said at least one second local area network and said at least one third local area network further comprises a corresponding one of at least one network switch for routing transaction data within said at least one second local area network and said at least one third local area network.

26. A method for central management, storage and verification of remotely captured paper transactions from checks comprising the steps of:

capturing an image of the paper transaction data at one or more remote locations said transaction data including a payer bank's identification number, a payer bank's routing number, a payer bank's routing information, a payer's account number, a payer's check, a payer bank's draft, a check amount, a payee bank's identification number, a payee bank's routing information, and a payee's account number; and sending a captured image of the paper transaction data;

managing the capturing and sending of the transaction data;

collecting, processing, sending and storing the transaction data at a central location;

managing the collecting, processing, sending and storing of the transaction data;

encrypting subsystem identification information and the transaction data; and

transmitting the transaction data and the subsystem identification information within and between the remote location(s) and the central location.

27. The method as in claim **26** wherein said managing the capturing and sending step comprises the steps of:

successively transforming the captured transaction data to a bitmap image, a compressed bitmap image, an encrypted, compressed bitmap image and an encrypted, compressed bitmap image tagged with information identifying a location and time of the transaction data capturing; and

storing the tagged, encrypted, compressed bitmap image.

28. The method as in claim **27** wherein said managing the capturing and sending step also captures electronic transactions from credit cards, smart cards and debit cards, signature data or biometric data, further comprising the steps of:

initiating an electronic transaction;

capturing signature data;

capturing biometric data; and

printing a paper transaction with data glyphs for the initiated electronic transaction.

29. A method as in claim **26** wherein:

said capturing and sending step occurs at a plurality of remote locations; and

said collecting, processing, sending and storing step occurs at a plurality of central locations.

30. A method as in claim **29** wherein said collecting, processing, sending and storing step comprises the steps of:

polling the remote locations for transaction data with servers at the central locations;

storing the transaction data at the central location in a memory hierarchy, said storing maintains recently accessed transaction data in a primary memory and other transaction data in a secondary memory; and

dynamically assigning the servers at the central location to receive portions of the transaction data for balancing the transaction data among the servers; and

generating reports from the transaction data and providing data to software applications.

31. A method as in claim **30** wherein said storing the transaction data step comprises the steps of:

partitioning the stored transaction data with predefined templates into panels; and

identifying locations of the panels.

32. A method as in claim **31** wherein said managing the collecting, processing, sending and storing of the transaction data step comprises correcting errors in the panels of stored transaction data.

33. A method as in claim **32** further comprising the steps of:

polling the remote locations for captured electronic data, captured signature data and captured biometric data with servers at the central locations; and

comparing the captured signature data and the captured biometric data to stored signature data and stored biometric data respectively for identification verification.

34. A method as in claim **32** wherein said transmitting the transaction data step comprises the steps of:

transmitting data within the remote locations;

transmitting data from each remote location to a corresponding central location; and

transmitting data within the central locations.

35. A method as in claim **34** wherein said transmitting data from each remote location to a corresponding central location step comprises the steps of:

connecting each remote location to a corresponding central location; and

connecting each central location to corresponding remote locations.

36. A method as in claim 29 further comprising the steps of:

collecting and sending the electronic or paper transaction data at intermediate locations;

managing the collecting and sending of the transaction data; and

transmitting the transaction data within the intermediate location and between the intermediate locations and the remote locations and the central locations.

37. A method as in claim 36 wherein said managing the collecting and sending step comprises the steps of:

polling the remote locations for transaction data with servers in the intermediate locations;

storing the transaction data in the intermediate locations in a useful form, said storing maintains the transaction data in a primary memory of a memory hierarchy and performs backup storage of the transaction data into a secondary memory of the memory hierarchy; and

dynamically assigning the servers to receive portions of the transaction data for balancing the transaction data among the servers.

38. The method as in claim 36 wherein said transmitting the transaction data step comprises the steps of:

transmitting data within the remote locations;

transmitting data from each remote location to a corresponding intermediate location;

transmitting data within the intermediate locations;

transmitting data from each intermediate location to corresponding central locations; and

transmitting data within the central locations.

39. A method as in claim 38 wherein said transmitting data from each remote location to corresponding intermediate locations step comprises the steps of:

connecting each remote location to a corresponding intermediate location; and

connecting the intermediate locations to corresponding remote locations.

40. A method as in claim 38 wherein said transmitting data from each intermediate location to corresponding central locations comprises the steps of:

connecting each intermediate location to an external communication network; and

connecting the corresponding central locations to the communication network.

41. A method as in claim 40 wherein said transmitting data from each intermediate location to corresponding central locations step further comprises the steps of:

packaging the transaction data into frames; and

transmitting the frames through the external communication network.

42. A system for central management, storage and report generation of remotely captured paper transactions from checks comprising:

one or more remote data access subsystems for capturing and sending paper transaction data and verifying transaction data from the checks comprising at least one imaging subsystem for capturing the checks and at least one data access controller for managing the capturing and sending of the transaction data;

at least one central data processing subsystem for processing, sending, verifying and storing the paper transaction data and the subsystem identification information comprising a management subsystem for managing the processing, sending and storing of the of the transaction data; and

at least one communication network for the transmission of the transaction data within and between said one or more data access subsystems and said at least one data processing subsystem, with the data access subsystem providing encrypted subsystem identification information and encrypted paper transaction data to the data processing subsystem.

43. A method for central management, storage and verification of remotely captured paper transactions from checks comprising the steps of:

capturing an image of the check at one or more remote locations and sending a captured image of the check;

managing the capturing and sending of the transaction data;

collecting, processing, sending and storing the transaction data at a central location;

managing the collecting, processing, sending and storing of the transaction data;

encrypting subsystem identification information and the transaction data;

verifying the transaction data from the check; and

transmitting the transaction data and the subsystem identification information within and between the remote location(s) and the central location.

* * * * *

U.S. DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

October 6, 2015
(Date)

THIS IS TO CERTIFY that the attached document is a list of the papers that comprise the record before the Patent Trial and Appeal Board (PTAB) for the *Covered Business Method Patent Review* proceeding identified below:

FIDELITY NATIONAL INFORMATION SERVICES,
Petitioner
v.

DATATREASURY CORP.,
Patent Owner

Case: CBM2014-00020
Patent 6,032,137

By authority of the

DIRECTOR OF THE UNITED STATES PATENT AND TRADEMARK OFFICE

Marcia L. Fletcher

Certifying Officer

Prosecution History CBM2014-00020

Date	Document
10/25/2013	Petition for Covered Business Method Patent Review
10/25/2013	Petitioner's Power of Attorney
10/31/2013	Notice of Filing Date Accorded to Petiton
11/15/2013	Patent Owner's Mandatory Notices
11/19/2013	Patent Owner's Power of Attorney
1/17/2014	Petitioner's Supplemental Mandatory Notices
2/1/2014	Patent Owner's Preliminary Response
2/10/2014	Order - Conduct of the Proceeding
2/12/2014	Patent Owner's Submission of Corrected Exhibits
3/26/2014	Petitioner's Second Supplemental Mandatory Notices
4/25/2014	Petitioner's Second Submission of Claim Scope Statement
4/29/2014	Decision - Institution of Covered Business Method Patent Review
4/29/2014	Scheduling Order
5/12/2014	Petitioner's Request for Rehearing
5/27/2014	Petitioner's List of Proposed Motions
5/27/2014	Patent Owner's List of Proposed Motions
6/2/2014	Petitioner's Request for Expedited Determination of Patentability
6/2/2014	Petitioner's Exhibit List
6/10/2014	Patent Owner's Opposition to Request for Expedited Determination
6/13/2014	Decision - Request for Rehearing
6/23/2014	Order - Conduct of the Proceedings
7/11/2014	Decision - Conduct of the Proceedings
7/29/2014	Patent Owner's Response to Petition
8/29/2014	Petitioner's Reply Brief
10/10/2014	Petitioner's Request for Oral Hearing
10/14/2014	Patent Owner's Request for Oral Argument
11/10/2014	Order - Trial Hearing
12/5/2014	Petitioner's Updated Exhibit List
12/5/2014	Patent Owner's Objection and Motion to Exclude
12/5/2014	Patent Owner's Notification of Participation
12/8/2014	Patent Owner's Withdrawal of Motion to Exclude
1/7/2015	Oral Hearing Transcript
4/29/2015	Final Written Decision
5/29/2015	Patent Owner's Updated Mandatory Notice
5/29/2015	Patent Owner's Appointment of Backup Counsel
5/29/2015	Patent Owner's Request for Rehearing
6/2/2015	Patent Owner's Request for Rehearing, Updated Mandatory Notices and Appointment of Backup Counsel
7/30/2015	Decision - Request for Rehearing

Trials@uspto.gov
571-272-7822

Paper 38
Entered: June 26, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FIDELITY NATIONAL INFORMATION SERVICES, INC.,
Petitioner,

v.

DATATREASURY CORP.,
Patent Owner.

Case CBM2014-00021
Patent 5,910,988

Before MICHAEL P. TIERNEY, WILLIAM V. SAINDON, and MATTHEW R. CLEMENTS, *Administrative Patent Judges*.

TIERNEY, *Administrative Patent Judge*.

DECISION
DataTreasury's Request for Rehearing
of Final Written Decision
37 C.F.R. § 42.71

I. STATEMENT OF THE CASE

On April 29, 2015, we entered a Final Written Decision in which we found claims 1–123 of U.S. Patent No. 5,910,988 ("the '988 Patent") to be unpatentable. Paper 34 ("Final Dec."). Patent Owner, DataTreasury Corp., has filed a request for rehearing of that decision. Paper 35 ("Req. Reh'g."). For the reasons discussed below, Patent Owner's Request for Rehearing is denied.

II. THE REQUEST FOR REHEARING

Patent Owner seeks reconsideration based on the following main contentions: (a)
the Board erred in determining that the '988 patent is a covered business method patent; (b) the Board erred in determining that the challenged claims are directed to patent ineligible subject matter; and (c) the Board erred in determining that the challenged claims lacked sufficient written description for encrypting the claimed subsystem identification information.

We have reviewed Patent Owner's request for rehearing and carefully considered Patent Owner's arguments. Our decision on rehearing addresses the main arguments presented by Patent Owner. We have, however, considered all of the arguments presented, including those not addressed specifically in this decision. We are not persuaded that the Board misapprehended or overlooked Patent Owner's arguments presented in its response or evidence with respect to the patentability of the challenged claims.

III. ANALYSIS

In pertinent part, 37 C.F.R. § 42.71(d) states:

> The burden of showing a decision should be modified lies with the party challenging the decision. The request must specifically identify all matters the party believes the Board misapprehended or overlooked, and the place where each matter was previously addressed in a motion, an opposition, or a reply.

Patent Owner's main arguments presented in its request for rehearing are addressed below.

A. The '988 patent is a Covered Business Method Patent

Patent Owner contends that the '988 patent is not eligible for covered business method review as the '988 patent is direct to "a specific data processing system that is application agnostic." Req. Reh'g. 2. Additionally, Patent Owner contends that the Board erred in holding that the '988 patent does not claim a technological invention. *Id*. at 4. We have considered Patent Owner's arguments but are not persuaded that we misapprehended or overlooked that the subject matter of the '988 patent is ineligible for covered business method review.

Our Decision to Institute (Paper 14) held that the '988 patent is directed to financial activity, processing financial transactions, and constitute a financial service or product. Dec. to Inst. 10–11. Patent Owner's contention that the '988 patent is application agnostic fails to address our prior finding that the patent states that it is directed to financial products and services by capturing an image of financial transaction data. *Id*.

Patent Owner cites the ’988 specification’s “Field of Invention” at column 1, lines 9–14 for the proposition that the data is not limited to a particular application. Req. Reh’g 2. Patent Owner however, overlooks the fact that the Field of the Invention section begins by stating:

> This invention relates generally to the automated processing of documents and electronic data from different applications including sale, business, banking and general consumer transactions.

Ex. 1001, 1:5–9. As apparent from the ’988 patent, the claimed data processing system is directed to a financial service or product.

Patent Owner also contends that the Board erred in holding that the ’988 patent does not claim a technological invention. Req. Reh’g. 4. According to Patent Owner, “[t]he [’988] Patent is directed to a new and distinct arrangement of computer components that transmit data in a new way.” *Id*. Patent Owner however, does not show where the Board erred in its Decision to Institute, which held that none of the steps of representative claim 26 recites a novel and unobvious technological feature. Dec. to Inst. 12. This holding was reaffirmed in the Final Written Decision. Final Dec. 10.

B. The Challenged Claims are Directed to Patent Ineligible Subject Matter

Patent Owner states that the Board erred in concluding that the ’988 patent claims fails to claim patent-eligible subject matter. Req. Reh’g. 4. According to Patent Owner, the Board improperly considered only one claim—claim 26—as representative, and failed to consider each of the 123 claims in the Patent. *Id*. at 5. For example, Patent Owner contends that the

Board did not address additional limitations, such as the card interface of claim 3, the tagged bitmap format images of claim 4, and the domain name assigning software of claim 9. *Id*. at 8. Additionally, Patent Owner also disputes the Board's determination that the claims are directed to an abstract idea, the determination that the claims improperly preempt the abstract idea, and the Board's failure to discuss both precedent and the '988 patent's tiered networked teachings. *Id*. at 4–11.

We have considered Patent Owner's contentions but do not find them persuasive. For example, although Patent Owner contends that the Board did not address certain limitations in its 123 challenged claims, Patent Owner does not identify where these particular limitations were discussed in its Patent Owner Response. Arguments not raised in the briefs before the Board and evidence not previously relied upon in the briefs are not permitted in the request for rehearing. Additionally, as stated in the Final Written Decision, the Board considered each of the challenged claims and was persuaded based on the evidence presented that the claims lacked limitations that meaningfully limited the abstract idea. Final Dec. 18. In particular, the Board credited the testimony of Petitioner's expert, Dr. Alexander, that the '988 patent claims merely arrange old, well-known elements with each performing the same function it had been known to perform. *Id*. Dr. Alexander's testimony addresses each of the now-disputed limitations, e.g., card interface (claim 3), tagged bitmap format images (claim 4), and domain name assigning software (claim 9) and demonstrates that the limitations merely recite a known set of prior art elements used according to their established functions. Ex. 1003 ¶¶ 104–138.

C. The Challenged Claims Lacked Sufficient Written Description

Patent Owner contends that Petitioner failed to prove that the '988 patent claims lack written description for "encrypting subsystem identification information" limitation in claims 1–41 and 51–69. Req. Reh'g. 11–15. According to the Patent Owner, the Board erroneously placed the burden of proof on the Patent Owner to demonstrate written description and disregarded the disclosure of the '988 patent that its system is capable of encrypting all of the transferred information. *Id*. Patent Owner cites the following phrase from the Final Written Decision: "to demonstrate that Patent Owner possessed the invention" as evidence that the Board placed the burden on the Patent Owner to prove written description. *Id*. at 12. To place the phrase in context, the Final Written Decision states:

> The claims require encrypting "subsystem identification information" and not merely "identification information." Patent Owner's citations to the '988 patent specification fail to demonstrate that Patent Owner possessed the invention. As recognized by Dr. Alexander, one skilled in the art would understand that the '988 patent specification does not describe any encryption to the tag headers that are prepended to the ECBI. Ex. 1003 ¶¶ 149–159.

Final Dec. 21–22. As apparent from the Final Written Decision, the burden of proof was placed on Petitioner. The Board credited the testimony of Petitioner's expert, Dr. Alexander, and held that Petitioner met its burden and demonstrated that the '988 patent does not describe encrypting all of the transferred information. Specifically, the Final Written Decision states:

> Based on the evidence of record, we credit the testimony of Dr. Alexander and agree with Petitioner that:
>
> (1) the specification fails to describe encrypting the DAT_TERMINAL_ID;

> (2) generic "identification information" does not constitute the claimed subsystem identification information; and
> (3) subsystem identification information is not included in the "paper transaction data" of the disclosed receipt.
>
> Reply 12–13. We find that Petitioner has demonstrated that claims 1–41 and 51–69 are unpatentable for lack of sufficient written description for encrypting subsystem identification information.

Final Dec. 22.

In consideration of the above, the Patent Owner's Request for Rehearing is DENIED.

CBM 2014-00021
Patent 5,910,988

For PETITIONER:

Erika H. Arner, Lead Counsel
Darren M. Jiron, Backup Counsel
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.
E-Mail FIS-Ballard@finnegan.com
erika.arner@finnegan.com
darren.jiron@finnegan.com

For PATENT OWNER:

Abraham Hershkovitz, Lead Counsel
Eugene C. Rzucidlo, Backup Counsel
HERSHKOVITZ & ASSOCIATES, PLLC
E-Mail AHershkovitz@Hershkovitz.net
E-Mail GRzucidlo@Hershkovitz.net

Trials@uspto.gov
571-272-7822

Paper 34
Entered: April 29, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FIDELITY NATIONAL INFORMATION SERVICES, INC.,
Petitioner,

v.

DATATREASURY CORP.,
Patent Owner.

Case CBM2014-00021
Patent 5,910,988

Before MICHAEL P. TIERNEY, WILLIAM V. SAINDON, and MATTHEW R. CLEMENTS, *Administrative Patent Judges*.

TIERNEY, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
Covered Business Method Patent Review
35 U.S.C. §328(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

Fidelity National Information Services, Inc. ("Fidelity" or "Petitioner") filed a petition ("Pet.") requesting review under the transitional program for covered business method patent review of claims 1–123 of U.S. Patent No. 5,910,988 ("the '988 patent") (Ex. 1001). On April 29, 2014, pursuant to 35 U.S.C. § 324, we instituted this trial as to claims 1–123 under 35 U.S.C. § 101 and claims 1–41 and 51–69 under 35 U.S.C. § 112, lack of written description (Paper 14, "Dec. to Inst."). Patent Owner DataTreasury Corp. ("Patent Owner" or "DataTreasury") filed a Patent Owner Response (Paper 25, "PO Resp."), and Petitioner filed a Reply (Paper 26, "Reply").

Patent Owner filed a Motion to Exclude Petitioner's demonstratives. Paper 32. Patent Owner subsequently withdrew its Motion to Exclude. Paper 33.

An oral hearing in this proceeding was held on December 9, 2014. A transcript of the hearing may be found in CBM2014-00020, Paper 33, "Tr.".

We have jurisdiction under 35 U.S.C. § 6(c). This Final Written Decision is issued pursuant to 35 U.S.C. § 328(a) and 37 C.F.R. § 42.73.

For the reasons that follow, we determine that Fidelity has shown by a preponderance of the evidence that claims 1–123 are unpatentable under 35 U.S.C. § 101 and claims 1–41 and 51–69 are unpatentable under 35 U.S.C. § 112, 1st paragraph,[1] for lack of written description.

---

[1] Section 4(c) of the Leahy-Smith America Invents Act ("AIA") re-designated 35 U.S.C. § 112 ¶ 1 as 35 U.S.C. § 112(a). Pub. L. No. 112-29, 125 Stat. 284, 296–07 (2011). Because the '988 patent has a filing date before September 16, 2012 (effective date of § 4(c)), we refer to the pre-AIA version of 35 U.S.C. § 112, in this Decision.

A. The ’988 Patent (Ex. 1001)

The ’988 patent is directed to a system for remote data acquisition, and centralized processing and storage of the acquired data. Ex. 1001, Abstract. An object of the invention is to provide an automated system to manage and store captured electronic and paper transactions from various activities including banking and consumer applications. *Id*. at 3:30–35. Generally, the ’988 patent describes scanning documents using a scanner attached to a general purpose network computer that is connected via a carrier cloud to a server that inserts images and data received into a database. *Id*. at Figs. 1–2, 3:30–51, 4:60–67, 5:40–45, 16:38–45. Additionally, the general purpose network computer encrypts the images and data to provide a system with maximal security. *Id*. at 3:30–35, 7:31–35, 8:3–5.

Figure 1 of the ’988 patent, provided below, depicts a preferred embodiment of the system having three major operational elements:

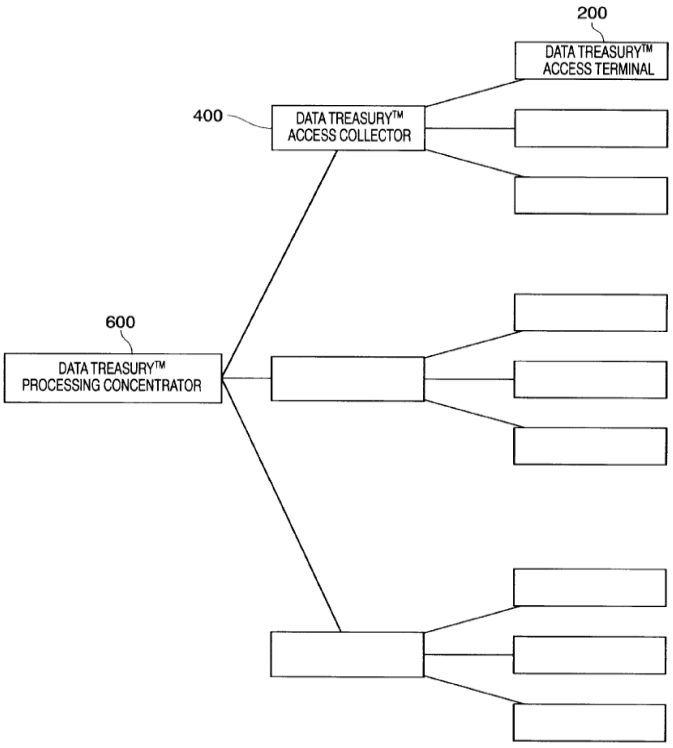


FIG. 1

The ’988 patent describes the tiered arrangement depicted in Figure 1 as follows:

> FIG. 1 shows the architecture of the DataTreasury™ System 100. The DataTreasury™ System 100 has three operational elements: the DataTreasury™ System Access Terminal (DAT) 200 (the remote data access subsystem), the DataTreasury™ System Access Collector (DAC) 400 (the intermediate data collecting subsystem), and the DataTreasury™ System Processing Concentrator (DPC) 600 (the central data processing subsystem).

Id. at 4:60–67.

Figure 2 of the ’988 patent, provided below, depicts a block diagram of the DAT (remote data access subsystem terminal):

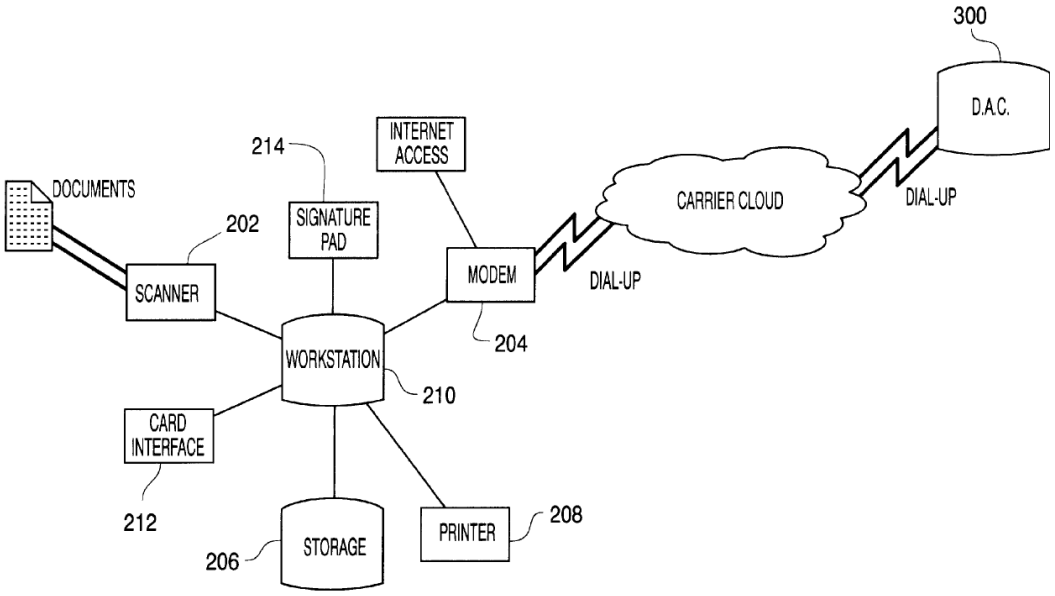


FIG. 2

As shown in Figure 2, scanner 202 is connected to workstation 210, which is connected to data system access collector 300. The workstation can be a general purpose computer and performs tasks including compressing, encrypting, and tagging a scanned bitmapped image. *Id*. at 5:40–45, 7:31–35.

The '988 patent is said to improve upon the prior art by providing an automated, reliable, secure system to process electronic and paper transactions. *Id*. at 3:25–29.

B. Illustrative Claims

Independent claims 26 and 46 are illustrative of the challenged claims in the '988 patent and are reproduced below:

> 26. A method for central management, storage and verification of remotely captured paper transactions from documents and receipts comprising the steps of:
>
> capturing an image of the paper transaction data at one or more remote locations and sending a captured images of the

transaction data;

managing the capturing and sending of the transaction data;

collecting, processing, sending and storing the transaction data at a central location;

managing the collecting, processing, sending and storing of the transaction data;

encrypting subsystem identification information and the transaction data; and

transmitting the transaction data and the subsystem identification information within and between the remote location(s) and the central location.

46. A method for transmitting data within and between one or more remote subsystems, at least one intermediate subsystem and at least one central subsystem in a tiered manner wherein each of the central subsystems communicate with at least one intermediate subsystem and each of the intermediate subsystems communicate with at least one remote subsystems comprising the steps of:

capturing an image of documents and receipts and extracting data therefrom;

transmitting data within the remote locations;

transmitting data from each remote location to corresponding intermediate location;

transmitting data within the intermediate locations;

transmitting data from each intermediate location to corresponding central locations; and

transmitting data within the central locations.

C. Related Proceedings

Petitioner indicates that the '988 patent is asserted in *DataTreasury Corp. v. Fidelity National Information Services, Inc*., No. 2:13-cv-432 (E.D. Tex.) in the U.S. District Court for the Eastern District of Texas ("the District Court"). Pet. 17. Petitioner also identifies an additional twenty-three district court proceedings involving the '988 patent. Pet. 4–6.

D. Alleged Grounds of Unpatentability Instituted in Trial

Petitioner contends that the challenged claims are unpatentable based on the following grounds:

Grounds	Claims Challenged
§ 101	1–123
§ 112, 1st paragraph, Written Description	1–41 and 51–69

II. ANALYSIS

A. Claim Construction

The Board interprets claims of unexpired patents using the "broadest reasonable construction in light of the specification of the patent in which [they] appear[]." 37 C.F.R. § 42.300(b); *see* Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,766 (Aug. 14, 2012) ("Trial Practice Guide"); *In re Cuozzo Speed Techs., LLC*, 778 F.3d 1271, 1281 (Fed. Cir. 2015); *In re Translogic Tech., Inc*., 504 F.3d 1249, 1257 (Fed. Cir. 2007); *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). Claim terms are given their plain and ordinary meaning as would be understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. "There are only two exceptions to this general rule: 1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution." *Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

In the Decision on Institution, we interpreted various claim terms of the '988 patent as follows:

Claim Term (Claims)	Interpretation
"encrypt" or "encrypting" (1, 4, 5, 26, 27, 120 and 123)	Convert into a form unreadable by anyone without a secret decryption key.
"within and between" (1, 26, 42, 46, 84, 88, 93, 97, 102, 106, 110, 114, 118, and 121)	Data is transmitted both within a given subsystem (i.e., between the various components comprising the subsystem or location) and between one subsystem or location to another subsystem or location.
"tiered manner" or "tiered architecture" (42, 46, 84, 88, 93, 97, 102, 106, 110, 114, 118, and 121)	The conceptual structure and logical organization of subsystems in a hierarchy of functional layers.

See Dec. to Inst. 7–9. The parties do not dispute these interpretations in their Patent Owner Response and Reply. We adopt the above claim constructions based on our previous analysis, and see no reason to deviate from those constructions for purposes of this decision.

B. Covered Business Method Patent

We determined, in the Decision on Institution, that the '988 patent is a covered business method patent as defined in § 18(a)(1)(E) of the AIA, and 37 C.F.R. § 42.301, because at least one claim of the '137 patent is directed to a covered business method. Dec. to Inst. 9–13.

The definition of "covered business method patent" in Section 18(d)(1) of the AIA excludes patents for "technological inventions." Patent Owner contends that the Board erred in instituting this proceeding alleging

that every claim of the ’988 patent recites a technological invention. PO Resp. 11–16.

Patent Owner states that every system claim and every subsystem claim in the ’137 patent is directed to technological equipment and provides a solution to the transmission of financial information. *Id*. at 13–14. Patent Owner further contends that every method claim recites steps performed by technological equipment. *Id*. at 14. The challenged claims however, merely require the use of “off the shelf” technology, including conventional imaging scanners attached to a general purpose computer network. *Id*. at 16; Declaration of Dr. Peter Alexander,[2] Ex. 1003 ¶¶ 105–138.

Patent Owner states that its system is a technological system because its claims are directed to a three-tiered system including three subsystems, which results in a technological banking system that is new, useful, and nonobvious. Paper 24, 15–16. Patent Owner fails to explain how a three-tier system is technological. For example, the three-tier system can be viewed as reflecting a banking system having networked branch offices, regional offices and a central home office.

We have considered Patent Owner’s remaining arguments and evidence regarding its contention that all the claims of the ’988 patent are directed to a technological invention but are not persuaded that its system and method claims recite a technological feature that is novel and unobvious over the prior art. We reaffirm our determination in the Decision to Institute

[2] We conclude that Dr. Alexander is qualified to testify as to the understanding of one skill in the art in this proceeding. *See* Ex. 1003 ¶¶ 1–4.

and conclude that the ’988 patent is eligible for a covered business method patent review.

C. Grounds Based on 35 U.S.C. § 101— Claims 1–123 Are Directed to Non-Statutory Subject Matter

Petitioner challenges claims 1–123 of the ’988 patent under 35 U.S.C. § 101, as directed to patent-ineligible subject matter. Pet. 21–39. Patent Owner disagrees and maintains that its claims are directed to patent-eligible processes because the claims do not recite an abstract idea. PO Resp. 31–62. For example, Patent Owner states:

> With respect to §101, the real issue in this CBM Proceeding is whether the teaching of scanning or imaging of documents and receipts is an “abstract idea.”

Id. at 48.

1. Section 101 Subject Matter Eligibility

For claimed subject matter to be patent eligible, it must fall into one of four statutory classes set forth in 35 U.S.C. § 101: a process, a machine, a manufacture, or a composition of matter. The Supreme Court recognizes three categories of subject matter that are ineligible for patent protection: “laws of nature, physical phenomena, and abstract ideas.” *Bilski v. Kappos*, 561 U.S. 593, 601 (2010) (internal quotations and citation omitted). A law of nature or an abstract idea by itself is not patentable; however, a practical application of the law of nature or abstract idea may be deserving of patent protection. *Mayo Collaborative Servs. v. Prometheus Labs., Inc*., 132 S. Ct. 1289, 1293–94 (2012). To be patentable, however, a claim must do more than simply state the law of nature or abstract idea and add the words “apply it.” *Id*.

In *Alice Corp. Pty, Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014), the Supreme Court recently clarified the process for analyzing claims to determine whether claims are directed to patent-ineligible subject matter. In *Alice*, the Supreme Court applied the framework set forth previously in *Mayo*, "for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of these concepts." *Alice*, 134 S. Ct. at 2355. The first step in the analysis is to "determine whether the claims at issue are directed to one of those patent-ineligible concepts." *Id*. If they are directed to a patent-ineligible concept, the second step in the analysis is to consider the elements of the claims "individually and 'as an ordered combination'" to determine whether there are additional elements that "'transform the nature of the claim' into a patent-eligible application." *Id*. (quoting *Mayo*, 132 S. Ct. at 1291, 1297). In other words, the second step is to "search for an 'inventive concept'—i.e., an element or combination of elements that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'" *Id*. (alteration in original) (quoting *Mayo*, 132 S. Ct. at 1294). Further, the "prohibition against patenting abstract ideas 'cannot be circumvented by attempting to limit the use of the formula to a particular technological environment' or adding 'insignificant postsolution activity.'" *Bilski*, 561 U.S. at 610–11 (quoting *Diamond v. Diehr*, 450 U.S. 175, 191–92 (1981)).

The patents at issue in *Alice* claimed "a method of exchanging financial obligations between two parties using a third-party intermediary to mitigate settlement risk." *Alice*, 134 S. Ct. at 2356. Like the method of hedging risk in *Bilski v. Kappos*, 561 U.S. at 628—which the Court deemed

"a method of organizing human activity"—*Alice*'s "concept of intermediated settlement" was held to be "'a fundamental economic practice long prevalent in our system of commerce.'" *Alice*, 134 S. Ct. at 2356. Similarly, the Court found that "[t]he use of a third-party intermediary . . . is also a building block of the modern economy." *Id*. "Thus," the Court held, "intermediated settlement . . . is an 'abstract idea' beyond the scope of § 101." *Id*.

2. DataTreasury's Challenged Claims Contain an Abstract Idea

a. Transferring information from one location to another where the transferred information is unreadable without a secret decoder key

Independent claim 26 is representative of the challenged claims. Claim 26 is directed to a method comprising capturing an image of documents and receipts and extracting data therefrom, and collecting, managing, encrypting subsystem identification information and the transaction data and transmitting the data to various locations within a system. Ex. 1001, 25:11–27. As apparent from claim 26, and identified in the Decision to Institute, Patent Owner's claims are, in substance, directed to the underlying idea of transferring information from one location to another where the transferred information is unreadable without a secret decoder key. Dec. to Inst. 19.[3]

Patent Owner contends that the challenged claims do not recite an abstract idea. Patent Owner argues that, unlike the algorithms in

[3] We note that claims 50 and 70–123 are even broader in that they do not require encryption (information unreadable without a secret decoder key).

Benson, encryption is patent eligible. For example, Patent Owner states:

> Encryption of data as a security measure is, in general, ubiquitous, and differs considerably from a mere mathematical algorithm or formula, and is accomplished not only in the '137 Patent, but is also accomplished in many patents, as discussed above. Class 705, Data Processing: Financial, Business Practice, Management, or Cost/Price Determination, includes a large number of patents that encrypt data in subclass 50 and subclasses that are indented under subclass 50.

PO Resp. 54. The fact that other patents have issued that relate to encrypted data fails to demonstrate that the basic concept of encryption is not abstract. An invention is not rendered ineligible for patent simply because it involves an abstract concept. *See Diamond* v. *Diehr*, 450 U.S. 175, 187 (1981).

We agree with Patent Owner that the basic concept of encryption is ubiquitous. Encryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years. Like hedging, encryption in its simplest form does not require the use of technology to communicate secure messages. Specifically, encryption, in its simplest form, could be performed with pencil and paper.

Patent Owner contends that there is no indication that patents employing encryption have been held to recite an abstract idea. PO Resp. 56. Patent Owner relies upon *TQP Development, LLC v. Intuit Inc.*, No. 2:12-CV-180, 2014 WL 651935 (E.D. Tex. Feb. 19, 2014), for the proposition that a general recitation of encryption renders the

claims patent eligible and that encryption is not an abstract idea. PO Resp. 58.

The *TQP* decision concerns a motion for summary judgment of invalidity of U.S. Patent No. 5,412,730, which alleged that the asserted claims were invalid as directed to patent-ineligible subject matter. *TQP*, 2014 WL 651935, at *3. Claim 1, the only asserted independent claim, related to a method of transmitting encrypted data. The method included the steps of providing a sequence of blocks in encrypted form by providing a seed value to a transmitter and a receiver, generating a first sequence of a pseudo-random key value based on the seed value, and encrypting the data sent. Additionally, the method required the generation of a second sequence of pseudo-random key values that are produced at a time dependent upon predetermined characteristics of the data transmitted, and decrypting the data in accordance with the second sequence. *Id*. at *1–*2.

The district court in *TQP* characterized the asserted claims as directed to a "statutory process" under § 101 and proceeded to the question of whether the recited claim raised "abstractness" problems, which the court characterized as posing a risk of preempting an abstract idea. *Id*. at *6. On this point, the court stated:

> Because the claim language is generic in nature—referring to a "transmitter," a "receiver," and a "communication link," rather than more specific structures, there would appear to be some risk of unacceptable preemption.

Id. Where a risk exists, the court stated that a determination needed to be made as to whether the claims contained additional substantive limitations such that, in practical terms, the claims do not cover the

full abstract idea itself. *Id*. at *5–*6. The court reviewed the claims and held that they were drawn to a very specific encryption method, added required steps to the core idea underlying the invention, and involved a way of making computer communication itself more effective by making that communication more secure. *Id*. at *7–*14. Further, the court determined that the motion for summary judgment raised factual issues. *Id*. at *10. Based on its review, the court denied the motion for summary judgment.

We hold, as did the court in *TQP*, that the challenged claims pose a risk of unacceptable preemption as the claim language is generic in nature—referring to capturing images, managing the transaction data, collecting the data, encrypting subsystem identification information and transaction data, and transmitting data within and between a remote location and a central location. Accordingly, we review the claims for an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the ineligible concept itself. *Mayo*, 132 S. Ct. at 1294.

b. Imaging or scanning documents

Patent Owner attempts to recast the identified abstract idea by focusing on the imaging and scanning concepts encompassed by the challenged claims. For example, Patent Owner states:

> With respect to §101, the real issue in this CBM Proceeding is whether the teaching of scanning or imaging of documents and receipts is an "abstract idea."

PO Resp. 48. Althoughwe have identified the abstract idea as involving the transfer of information from one location to another where the transferred information is unreadable without a secret decoder key, we address Patent Owner's arguments concerning the abstractness of imaging and scanning to the extent the arguments may be of general applicability.

i. Routine business practices can be abstract

Patent Owner contends that the imaging of documents and receipts is not an abstract idea or concept. PO Resp. 39–40. According to Patent Owner, scanning or imaging documents is routine in banking and financial patents, and not abstract. *Id*. Patent Owner also states that scanning or imaging a document is not an abstract idea contending "[i]nstead, it is a practice that is essentially universal, especially in business environments such as banking or financial businesses." *Id*. at 40. The fact that a business practice is used widely does not preclude a determination that the underlying practice involves an abstract idea. For instance, risk hedging (*Bilski*) and intermediated settlement (*Alice*) are also routine business practices, but these practices have been held abstract.

ii. Presence of tangible objects does not foreclose abstractness

Patent Owner contends that imaging or scanning a check is not an abstract idea because documents and receipts are concrete objects. *Id*. at 44–45. The fact that a claim recites substantial physical limitations does not preclude a determination that the claim is effectively an unpatentable law of nature or an attempt to preempt an abstract idea. *Mayo*, 132 S. Ct. at 1297.

3. DataTreasury's Challenged Claims Do Not Contain Significant Meaningful Limitations Beyond the Abstract Idea

Petitioner contends that the '988 patent claims, when considered as a whole, fail to add anything significant to the underlying abstract idea. Pet. 23. Specifically, Petitioner states that the challenged claims add only well-known computer and imaging components in connection with the commonly-known multiple "tier" architecture. *Id*. at 23–24.

Petitioner identifies claim 46 as representative and states that the claim merely recites a method comprising the steps of capturing a check image, sending the image within and between various locations within a system. *Id*. at 25. Petitioner relies upon the testimony of Dr. Peter Alexander to support its contention that the claim adds nothing more than an arrangement of generic computer components and processes that were known to those of ordinary skill in the art, to the underlying abstract idea. Ex. 1003 ¶¶ 31–77, 105–138.

Patent Owner disagrees, and contends that claim 46 recites specific structural components that are cooperating subsystems that transmit data within and between one or more remote subsystems. PO Resp. 62–63. Patent Owner states that the specific structural components that are described in claim 46 accomplish the specific method steps of transmitting data and give life and meaning to the claim. *Id*. at 63–64.

We select independent claim 26 as illustrative of the challenged claims as opposed to independent claim 46, as claim 26 further requires encrypting subsystem identification information and the transaction data in addition to transmitting data. The apparatus and method steps recited in

claim 26 do not limit the claim in a meaningful way to avoid unacceptable preemption of the abstract idea. Patent Owner recognizes that encryption of data as a security measure is, in general, "ubiquitous." *Id*. at 54. Patent Owner also acknowledges that the subsystems recited in the challenged claims are composed of "off the shelf" technology. *Id*. at 16. Patent Owner also states that the claims do not claim any "particular" machines or components, as the invention is in the configuration of the system built from various components. Prelim. Resp. 32.

As to the "three-tier" architecture,[4] Dr. Alexander testifies that such architecture was known in the art. For example, Dr. Alexander cites U.S. Patent No. 5,373,550 to Campbell (Exhibit 1023), as describing tiered architecture with imaged checks being routed through network, such as that recited in the challenged claims. Ex. 1003 ¶¶ 208–215. Patent Owner acknowledges that the Campbell patent cited by Dr. Alexander was "old and well known long prior to the issue date of the involved patent. PO Resp. 15. We credit Dr. Alexander's testimony and find that three-tier architecture was conventional in the banking and financial services industry.

We credit Dr. Alexander's testimony and determine that the '988 patent simply arranges old well-known elements with each performing the same function it had been known to perform. *E.g.*, Ex. 1003 ¶¶ 26–28, 31, 85. Based on the record presented, we do not see how the limitations in claim 46 are significant meaningful limitations that transform the abstract

[4] Petitioner contends that the challenged claims do not recite a "three-tiered" architecture. Reply 8. For purposes of this decision, we assume the Patent Owner is correct in stating that its claims require such architecture.

idea into patent-eligible applications of these abstractions. Patent Owner's contentions focused on the alleged meaningful limitations appearing in claim 46 or the challenged claims in general. We have reviewed the remaining challenged claims and likewise are persuaded, based on the evidence presented, that the remaining claims also lack limitations that meaningfully limit the abstract idea and avoid unacceptable preemption. Reply, 1. We hold that the challenged claims recite nothing more than conventional equipment and steps, specified at a high level of generality on top of the underlying abstract concept. *Mayo*, 132 S. Ct. at 1300.

We note that Patent Owner states that imaging or scanning a document would transform the paper document into an image on film, or into data, and would satisfy the machine-or-transformation test. PO Resp. 40. Patent Owner however, also states that the machine-or-transformation test "does not have any applicability in this proceeding." *Id.* at 38. The challenged claims as a whole, however, do not result in any transformed articles. Rather, transaction (financial) data are duplicated, organized, and moved from one place to another. Ex. 1003 ¶¶ 139–141. Further, the fact that the claims involve the use of generic, well-known machines does not impart patentability under the machine-or-transformation test. *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972) (invalidating as patent-ineligible claimed processes that "can be carried out in existing computers long in use, no new machinery being necessary"). Simply appending conventional steps, specified at a high level of generality is not enough to supply an inventive concept and transform and otherwise patent-ineligible abstract idea into a patent-eligible subject matter.

We hold that the additional limitations in Patent Owner's claims that

seek to narrow the application of the abstract idea are merely an attempt to limit the use of the abstract idea to a particular field of use or add token postsolution components, which has long been held insufficient to save a claim in this context. *See Alice*, 134 S. Ct. at 2358; *Mayo*, 132 S. Ct. at 1294; *Bilski*, 561 U.S. at 610–11; *Diehr*, 450 U.S. at 191. We hold that Petitioner has shown by a preponderance of the evidence that claims 1–123 of the '988 patent are unpatentable under 35 U.S.C. § 101.

D. Grounds Based on 35 U.S.C. § 112, 1st Paragraph, Written Description—Claims 1–41 and 51–69

Petitioner contends that claims 1–41 and 51–69 are unpatentable under 35 U.S.C. 112, 1st paragraph, written description, because the '988 patent specification lacks sufficient disclosure that would have indicated to one of ordinary skill in the art that patentee possessed the claimed invention. Pet. 40–48. In particular, Petitioner contends that the '988 patent specification fails to describe "encrypting subsystem identification information." *Id*. Specifically, independent claims 1 and 26 require two different types of encrypted information: 1) encrypted paper transaction data, and 2) encrypted subsystem identification information. According to Petitioner, the '988 patent specification discloses that a compressed bitmap image (CBI) is encrypted (ECBI) and that a tag is prepended to the ECBI to form a tagged encrypted compressed bitmap image (TECBI). Pet. 42. Petitioner states that the '988 patent specification suggests that the tag prepended to the ECBI remains unencrypted. Pet. 42–43. Petitioner, and Dr. Alexander, conclude that the specification suggests that that subsystem identification information remains unencrypted. Pet. 43–44; Ex. 1003 ¶¶ 143, 149–158, 183. Patent Owner disagrees. PO Resp. 64–67.

Patent Owner directs our attention to column 6, line 30 of the '988 patent specification,[5] which states that the DAT card retrieves identification information for subsequent transmission. PO Resp. 65. Patent Owner also directs our attention to column 10, lines 58–67 of the specification, which provides that the DataTreasury System 100 can process receipts with alternate form as long as the receipt contains the appropriate information. *Id*. at 65. Patent Owner, from these cited passages, states that it is spelled out for one of ordinary skill in the art that the specification supports the encrypting subsystem identification information claim limitation. *Id*. at 67.

The test for written description is an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art. Using this test, the invention must be described in a manner sufficient to demonstrate that the inventor actually invented the claimed invention. *Ariad Pharm. Inc. v. Eli Lilly & Co*., 598 F.3d 1336 (Fed. Cir. 2010). "One shows that one is 'in possession' of the invention by describing the invention, with all its claimed limitations, not that which makes it obvious." *Lockwood v. Am. Airlines, Inc*., 107 F.3d 1565, 1571 (Fed. Cir. 1997). Written description is a question of fact judged as of the relevant filing date. *Falko-Gunter Falkner v. Inglis*, 448 F.3d 1357, 1363 (Fed. Cir. 2006).

The claims require encrypting "subsystem identification information" and not merely "identification information." Patent Owner's citations to the

[5] For purposes of this decision we assume that the cited portions of the '988 patent specification appear verbatim in the originally filed specification of U.S. Application No. 08/917,761, from which the '988 patent issued.

'988 patent specification fail to demonstrate that Patent Owner possessed the invention. As recognized by Dr. Alexander, one skilled in the art would understand that the '988 patent specification does not describe any encryption to the tag headers that are prepended to the ECBI. Ex. 1003 ¶¶ 149–159. Specifically, the '988 patent specification discloses a data access terminal (DAT) having a scanner that is used to scan a financial document, such as a receipt, to create a bitmap image of the document, which can then be compressed. Ex. 1001, 7:52–60, Fig. 2. The specification states that the DAT can use well-known encryption algorithms to encrypt the compressed bitmapped image. *Id*. at 8:3–5. The specification further discloses that once the ECBI has been generated, a tag is prepended to the ECBI to form the TECBI. *Id*. at 8:14–17. This process of forming a TECBI is depicted in Fig. 3A, which provides a flowchart of the process with the tag being added after the ECBI has been encrypted.

Based on the evidence of record, we credit the testimony of Dr. Alexander and agree with Petitioner that:

> (1) the specification fails to describe encrypting the DAT_TERMINAL_ID;
> (2) generic "identification information" does not constitute the claimed subsystem identification information; and
> (3) subsystem identification information is not included in the "paper transaction data" of the disclosed receipt.

Reply 12–13. We find that Petitioner has demonstrated that claims 1–41 and 51–69 are unpatentable for lack of sufficient written description for encrypting subsystem identification information.

III. CONCLUSION

We conclude Petitioner has proven, by a preponderance of the evidence, that claims 1–123 of the '988 patent are unpatentable under 35 U.S.C. § 101 and that claims 1–41 and 51–69 of the '988 patent are unpatentable under 35 U.S.C. § 112, 1st Paragraph, for lack of written description.

IV. ORDER

For the reasons given, it is hereby:

ORDERED that Petitioner has established by a preponderance of the evidence that claims 1–123 of the '988 patent are unpatentable;

FURTHER ORDERED that because this is a Final Written Decision, parties to the proceeding seeking judicial review of the Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

CBM 2014-00021
Patent 5,910,988

For PETITIONER:

Erika H. Arner, Lead Counsel
Darren M. Jiron, Backup Counsel
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.
11955 Freedom Drive
Reston, VA 20190
E-Mail Erika.Arner@finnegan.com
E-Mail Darren.Jiron@finnegan.com
Telephone 571-203-2700

For PATENT OWNER:

Abraham Hershkovitz, Lead Counsel
Eugene C. Rzucidlo, Backup Counsel
HERSHKOVITZ & ASSOCIATES, PLLC
2845 Duke Street
Alexandria, VA 22314
E-Mail AHershkovitz@Hershkovitz.net
E-Mail GRzucidlo@Hershkovitz.net
Telephone 703-370-4800

Trials@uspto.gov
571-272-7822

Paper 14
Entered: April 29, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FIDELITY NATIONAL INFORMATION SERVICES, INC.,
Petitioner,

v.

DATATREASURY CORP.,
Patent Owner.

Case CBM2014-00021
Patent 5,910,988

Before MICHAEL P. TIERNEY, WILLIAM V. SAINDON, and MATTHEW R. CLEMENTS, *Administrative Patent Judges*.

TIERNEY, *Administrative Patent Judge*.

DECISION
Institution of Covered Business Method Patent Review
37 C.F.R. § 42.208

I. INTRODUCTION

Fidelity National Information Services, Inc. ("Fidelity" or "Petitioner") filed a petition ("Pet.") on October 25, 2013 to institute a covered business method patent review of claims 1-123 of U.S. Patent No. 5,910,988 (Ex. 1001, "the '988 patent"). Paper 2. DataTreasury Corp. ("Patent Owner" or "DataTreasury") filed a preliminary response ("Prelim. Resp.") to the petition on January 31, 2014. We have jurisdiction under 35 U.S.C. § 324. *See* Section 18(a) of the Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284, 329 (2011) ("AIA").

The standard for instituting a covered business method patent review is set forth in 35 U.S.C. § 324(a), which provides as follows:

> THRESHOLD.—The Director may not authorize a post-grant review to be instituted unless the Director determines that the information presented in the petition filed under section 321, if such information is not rebutted, would demonstrate that it is more likely than not that at least 1 of the claims challenged in the petition is unpatentable.

Upon consideration of the information presented, we grant the petition, because Petitioner has demonstrated that claims 1-123 are more likely than not unpatentable under 35 U.S.C. § 101, and claims 1-49 and 51-69, are more likely than not, unpatentable under 35 U.S.C. § 112 for lack of written description.

A. Related Proceedings

Petitioner indicates that the '988 patent is asserted in a litigation titled *DataTreasury Corp. v. Fidelity National Information Services, Inc*., No. 2:13-cv-432 (E.D. Tex). Pet. 17. Petitioner also identifies an additional twenty-three district court proceedings involving the '988 patent. Pet. 4-6.

B. The '988 Patent (Ex. 1001)

The '988 patent is directed to a system for remote data acquisition and centralized processing and storage of the acquired data. Ex. 1001, Abstract. An object of the invention is to provide an automated system to manage and store captured electronic and paper transactions from various activities including banking and consumer applications. *Id*. at 3:30-35. Generally, the '988 patent describes scanning documents using a scanner attached to a general purpose network computer that is connected via a carrier cloud to a server that inserts images and data received into a database. *Id*. at Figs. 1-2, 3:30-51, 4:60-67, 5:40-45, 16:38-45. Additionally, the general purpose network computer encrypts the images and data to provide a system with maximal security. *Id*. at 3:30-35, 7:31-35, 8:3-5.

Figure 1 of the '988 patent, provided below, depicts a preferred embodiment of the system having three major operational elements:

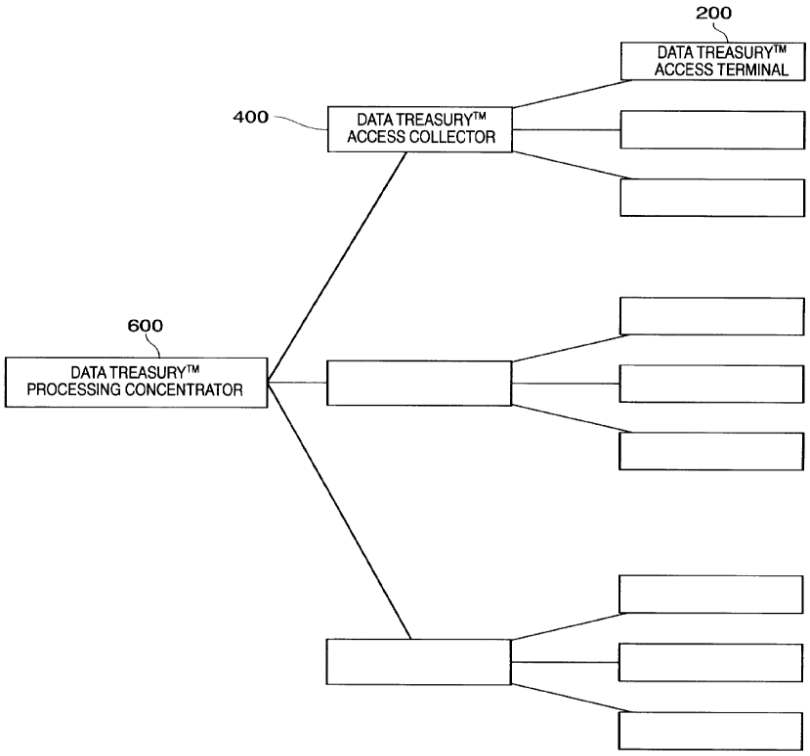


FIG. 1

The ’988 patent describes the tiered arrangement depicted in Figure 1 as follows:

> FIG. 1 shows the architecture of the DataTreasury™ System 100. The DataTreasury™ System 100 has three operational elements: the DataTreasury™ System Access Terminal (DAT) 200 (the remote data access subsystem), the DataTreasury™ System Access Collector (DAC) 400 (the intermediate data collecting subsystem), and the DataTreasury™ System Processing Concentrator (DPC) 600 (the central data processing subsystem).

Id. at 4:60-67.

Figure 2 of the ’988 patent, provided below, depicts a block diagram of the DAT (remote data access subsystem terminal):

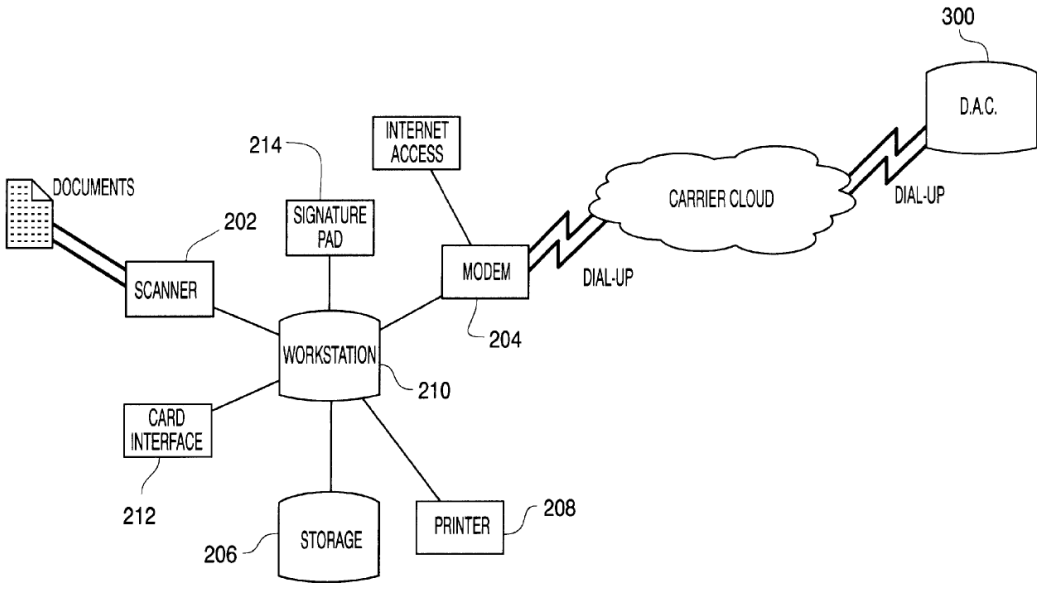


FIG. 2

As shown in Figure 2, a scanner 202 is connected to a workstation 210, which is connected to a data system access collector 300. The workstation can be a general purpose computer and performs tasks including compressing, encrypting and tagging a scanned bitmapped image. *Id*. at 5:40-45 and 7:31-35.

The ’988 patent is said to improve upon the prior art by providing an automated, reliable, secure system to process electronic and paper transactions. *Id*. at 3:25-29.

C. Exemplary Claims

Independent claims 26 and 42 are representative of the challenged claims in the ’988 patent and are reproduced below:

> 26. A method for central management, storage and verification of remotely captured paper transactions from documents and receipts comprising the steps of:
>
> capturing an image of the paper transaction data at one or more remote locations and sending a captured images of the transaction data;
>
> managing the capturing and sending of the transaction data;
>
> collecting, processing, sending and storing the transaction data at a central location;
>
> managing the collecting, processing, sending and storing of the transaction data;
>
> encrypting subsystem identification information and the transaction data; and
>
> transmitting the transaction data and the subsystem identification information within and between the remote location(s) and the central location.
>
> 42. A communication network for the transmission of data within and between one or more remote data processing subsystems, at least one intermediate data collecting subsystem and at least one central subsystem forming a tiered architecture wherein each of said at least one central data processing subsystem communicate with a corresponding some of said at least one data collecting subsystem and each of said at least one data collecting subsystem communicate with a corresponding some of said one or more data processing subsystems, said data processing subsystem including an imaging subsystem for capturing images of documents and receipts, comprising:

at least one first local area network for transmitting data within a corresponding one of said one or more remote subsystems;

at least one second local area network for transmitting data within a corresponding one of said at least one intermediate subsystem;

at least one third local area network for transmitting data within a corresponding one of said at least one central subsystem; and

at least one wide area network for transmitting data between said one or more remote subsystems, said at least one intermediate subsystem and said at least one central subsystem.

D. The Asserted Grounds

Petitioner contends that the challenged claims are unpatentable based on the following grounds:

Grounds	Claims Challenged
§ 112, Indefiniteness	42-51 and 70-123
§ 112, Written Description	1-123
§ 101	1-123

II. ANALYSIS

A. Claim Construction

Consistent with the statute and legislative history of the AIA, the Board interprets claims of an unexpired patent using the broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.300(b); *see also* Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,766 (Aug. 14, 2012). Moreover, claim terms are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art at the time of the invention and in the context of the patent disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir.

2007). An inventor may rebut the presumption that claim terms are given their ordinary and customary meaning by providing a definition of the term in the specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

Petitioners seek construction of three claim terms. Pet. 18-21. Patent Owner did not propose alternate constructions.

1. "Encrypt" or "Encrypting" (claims 1, 4, 5, 26, 27, 120, and 123)

The claim term "encrypt" or "encrypting" is recited in claims 1, 4, 5, 26, 27, 120, and 123. Petitioner proposes that encrypt or encrypting be construed as "convert into a form unreadable by anyone without a secret decryption key." Pet. 19. (citing Ex. 1003, Declaration of Dr. Peter Alexander,[1] ¶¶ 84, 85.).

The '988 patent describes its encryption algorithm as one that would be well known to an artisan of ordinary skill. Ex. 1001 at 8:3-5, Ex.1002 at 8:10-12. In previous district court litigation, encrypt was construed to mean "transformation of data into a form unreadable by anyone without a secret decryption key." Ex. 1017, 58-59. Dr. Alexander, however, testifies that the broadest reasonable construction would not be limited to taking action on "data." Ex. 1003 ¶ 86. Dr. Alexander also testifies that encryption must keep the content the same, even though the resulting form may be different, and thus the underlying information is not transformed as required by the district court construction. Ex. 1003 ¶ 87.

[1] We conclude that Dr. Alexander is qualified to testify as to the understanding of one skill in the art in this proceeding. *See* Ex. 1003 ¶¶ 1-4.

Based upon the record presented, we credit Dr. Alexander's Declaration and, for purposes of this Decision to Institute for the '988 patent, adopt Petitioner's proposed construction.

2. *"Within and Between" (claims 1, 26, 42, 46, 84, 88, 93, 97, 102, 106, 110, 114, 118 and 121)*

The claim term "within and between" is recited in claims 1, 26, 42, 46, 84, 88, 93, 97, 102, 106, 110, 114, 118 and 121. Petitioner contends that the broadest reasonable interpretation of this terminology is data is transmitted both within a given subsystem (i.e., between the various components comprising the subsystem or location) and between one subsystem or location to another subsystem or location. Pet. 19-21. Petitioner's proposed claim construction is identical to the District Court's Claim Construction Order in *DataTreasury Corp. v. Wells Fargo & Co.* No: 2:05-cv-291 (E.D. Tex. Mar. 11, 2009). Dr. Alexander testifies that the District Court's construction is consistent with the plain meaning as understood by one of ordinary skill in the art. Ex. 1003 ¶¶ 92, 94-95).

Based upon the record presented, we credit Dr. Alexander's Declaration and, for purposes of this Decision to Institute for the '988 patent, adopt the District Court's proposed construction, which is advanced by the Petitioner.

3. *"Tiered Manner/Tiered Architecture" (claims 42, 46, 84, 88, 93, 97, 102, 106, 110, 114, 118, 121)*

The claim term "tiered manner" is recited in claims 46, 88, 97, 106, 114, and 121, and the term "tiered architecture" is recited in claims 42, 84, 93, 102, 110, and 118. Petitioner argues that these terms should be construed to mean "the conceptual structure and logical organization of subsystems in a hierarchy of functional layers." Pet. 19, 21. This

construction is consistent with the '988 patent specification, which describes the embodiment depicted in Figure 1 as having "tiers" arranged in a hierarchy according to functions. Ex. 1001, 5:1-9.

Based upon the record presented, we adopt Petitioner's construction, as it is consistent with the '988 patent specification.

B. Standing for Covered Business Method Review of the '988 Patent

The parties disagree as to whether Petitioner has standing to file a petition for a covered business method review of the '988 patent. *See* Pet. 7-17; Prelim. Resp. 10-16. Section 18 of the AIA provides for the creation of a transitional program for reviewing covered business method patents. A "covered business method patent" is a patent that "claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service, except that the term does not include patents for technological inventions." AIA § 18(d)(1); *see* 37 C.F.R. § 42.301(a). To determine whether a patent is eligible for a covered business method patent review, the focus is on the claims. *See* Transitional Program for Covered Business Method Patents—Definitions of Covered Business Method Patent and Technological Invention; Final Rule, 77 Fed. Reg. 48,734, 48,736 (Aug. 14, 2012). A patent need have only one claim directed to a covered business method to be eligible for review. *Id*.

1. Sued for Infringement of the '988 Patent

The AIA requires that "[a] person may not file a petition for a transitional proceeding unless the person or the person's real party in interest or privy has been sued for infringement of the patent or has been charged

with infringement under that patent." AIA § 18(a)(1)(B); *see also* 37 C.F.R. § 42.302(a).

As discussed above, Petitioner represents that it has been sued for infringement of the '988 patent in *DataTreasury Corp. v. Fidelity National Information Services, Inc.*, No. 2:13-cv-432 (E.D. Tex). Thus, Petitioner has been sued for infringement for purposes of AIA § 18(a)(1)(B).

2. Financial Product or Service

A "covered business method patent" is a patent that "claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service, except that the term does not include patents for technological inventions." AIA § 18(d)(1); *see* 37 C.F.R. § 42.301(a) (emphasis added).

In promulgating rules for covered business method reviews, the Office considered the legislative intent and history behind the AIA's definition of "covered business method patent." *See* Transitional Program for Covered Business Method Patents—Definitions of Covered Business Method Patent and Technological Invention; Final Rule, 77 Fed. Reg. 48,734, 48,735-36 (Aug. 14, 2012). The "legislative history explains that the definition of covered business method patent was drafted to encompass patents 'claiming activities that are financial in nature, incidental to a financial activity or complementary to a financial activity.'" *Id*. (citing 157 Cong. Rec. S5432 (daily ed. Sept. 8, 2011) (statement of Sen. Schumer)). The legislative history indicates that "financial product or service" should be interpreted broadly. *Id*.

The ’988 patent describes capturing an image of financial transaction data, including sale, business, banking, and general consumer transactions, and transmitting the image to a storage facility, where the information about the financial transaction is recorded and stored. Ex. 1001, Abstract, 3:30-57. For example, claim 26 is directed to a “method for ,central management, storage and verification of remotely captured paper transactions from documents and receipts.” We determine that such activity falls within a financial product or service as it is directed to a financial activity, namely processing financial transactions (checks).

Based on the foregoing, the ’988 patent claims methods that are directed to a financial activity—processing financial transactions—that constitutes a financial product or service under § 18(d)(1).

3. Technological Invention

The definition of “covered business method patent” in Section 18(d)(1) of the AIA excludes patents for “technological inventions.” In determining whether a patent is for a technological invention, we consider “whether the claimed subject matter as a whole recites a technological feature that is novel and unobvious over the prior art; and solves a technical problem using a technical solution.” 37 C.F.R. § 42.301(b). The following claim drafting techniques, for example, typically do not render a patent a “technological invention”:

> (a) Mere recitation of known technologies, such as computer hardware, communication or computer networks, software, memory, computer-readable storage medium, scanners, display devices or databases, or specialized machines, such as an ATM or point of sale device.

> (b) Reciting the use of known prior art technology to accomplish a process or method, even if that process or method is novel and non-obvious.
>
> (c) Combining prior art structures to achieve the normal, expected, or predictable result of that combination.

Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,763-64 (Aug. 14, 2012).

Petitioner contends that the '988 patent claims fail to recite a novel and unobvious technological feature. Pet. 11-15. Patent Owner disagrees and states that the '988 patent is directed to a technological data processing system that performs a technological method driven by that technological data processing system. Prelim. Resp. 15.

We exercise our discretion and analyze claim 26 of the '988 patent to determine whether it recites a novel and unobvious technological feature. Claim 26 is directed to a method for central management, storage and verification of remotely captured paper transactions. The method requires the steps of capturing an image of paper transaction data, where the image may be captured using a conventional scanner. The transaction data are transferred from a remote location. The transaction data are managed, collected, processed, sent and stored at a central location. The subsystem identification information and transaction data are then encrypted, which can be done using a conventional algorithm. The transaction data and subsystem identification information are transmitted within and between the remote location and central location. None of the steps in claim 26 recites a novel and unobvious technological feature. Ex. 1003 ¶¶ 105-111. This is consistent with the description in the '988 patent specification and confirmed by the inventor of the '988 patent, who testified that he did not

actually create hardware when he came up with the invention. Ex. 1013, 63:15-24.

Based on the foregoing, we conclude that claim 26 of the '988 patent is not a technological invention under § 18(d)(1). Additionally, we conclude that the '988 patent is eligible for a covered business method patent review.

C. Grounds Based on 35 U.S.C. § 112, 2nd Paragraph, Indefiniteness—Claims 42-51 and 70-123

Petitioner contends that claims 42-51 and 70-123 are unpatentable under 35 U.S.C. § 112, 2nd paragraph, because they are indefinite. Pet. 51-56. Patent Owner disagrees. Prelim. Resp. 44-52.

Upon review of Petitioner's analysis and evidence, we determine that Petitioner has not demonstrated that claims 42-51 and 70-123 are more likely than not unpatentable for being indefinite.

The scope of the claims must be sufficiently definite to inform the public of the bounds of the protected invention, i.e., what subject matter is covered by the exclusive rights of the patent. *Halliburton Energy Servs. v. M-I, LLC*, 514 F.3d 1244, 1249 (Fed. Cir. 2008). The test for whether a claim meets the definiteness requirement is whether a person of ordinary skill in the art would have understood the scope of the claim when read in light of the specification. *Exxon Research & Eng'g Co. v. U. S.*, 265 F.3d 1371, 1375 (Fed. Cir. 2001); *Personalized Media Commc'ns v. Int'l Trade Comm'n*, 161 F.3d 696, 705 (Fed. Cir. 1998).

1. "Said Data Processing System"

Claim 42 recites "said data processing system" and claims 43-45 and 70-74 depend from claim 42. Petitioner states that the phrase "said data processing system" is ambiguous as there is more than one data processing

system present in claim 42. Pet. 51-52. Patent Owner contends that the phrase is definite as it is clear to one of ordinary skill in the art. Prelim. Resp. 49.

We agree with Patent Owner that one skilled in the art would understand that the phrase "said data processing system" refers to the remote data processing subsystem. Specifically, the preamble of claim 42 states "said data processing subsystem including an imaging subsystem for capturing images of documents and receipts." As depicted in Fig. 2, the remote data processing subsystem includes the imaging subsystem (scanner) for capturing images.

2. *"Tiered Architecture" and "Tiered Manner"*

Petitioner contends that Patent Owner failed to describe the boundaries of the claimed "tiered architecture" and "tiered manner" relative to the prior art and that claims 42-51 and 70-123, which include at least one of these terms, are invalid as indefinite. Pet. 53. Patent Owner disagrees and identifies Fig. 1 as depicting the tiered architecture, and that the tiers are described in the '988 patent. Prelim. Resp. 50.

We agree with Patent Owner. The '988 patent describes the use of tiers (bottom tier, next tier, top tier) and depicts the use of tiers. Ex. 1001, Fig. 1 and 5:1-9.

D. *Grounds Based on 35 U.S.C. § 112, 1st Paragraph, Written Description—Claims 1-123*

Petitioner contends that claims 1-123 are unpatentable under 35 U.S.C. 112, 1st paragraph, written description, because the '988 patent specification lacks sufficient disclosure that would have indicated to one of

ordinary skill in the art that patentee possessed the claimed invention. Pet. 40-51.

The test for written description is an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art. Using this test, the invention must be described in a manner sufficient to demonstrate that the inventor actually invented the claimed invention. *Ariad Pharm. Inc. v. Eli Lilly & Co.*, 598 F.3d 1336 (Fed. Cir. 2010). "One shows that one is 'in possession' of the invention by describing the invention, with all its claimed limitations, not that which makes it obvious." *Lockwood v. Am. Airlines, Inc.*, 107 F.3d 1565, 1571 (Fed. Cir. 1997).

1. *Encrypted/Encrypting Subsystem Identification Information*

Petitioner contends that claims 1-41 and 51-69 are unpatentable for lack of written description. Pet. 40-48. Specifically, independent claims 1 and 26 require two different types of encrypted information: 1) encrypted paper transaction data, and 2) encrypted subsystem identification information. According to Petitioner, the '988 patent specification discloses that a compressed bitmap image (CBI) is encrypted (ECBI) and that a tag is prepended to the ECBI to form a tagged encrypted compressed bitmap image (TECBI). Pet. 42. Petitioner states that the '988 patent specification suggests that the tag prepended to the ECBI remains unencrypted. Pet. 43. Patent Owner disagrees contending that encrypting subsystem information refers to encrypting identification information, such as that found on a sales receipt. Prelim. Resp. 39-42.

Dr. Alexander testifies that one skilled in the art would understand that the '988 patent specification does not describe any encryption to the tag

headers that are prepended to the ECBI. Ex. 1003 ¶¶ 149-159. Specifically, the '988 patent specification discloses a data access terminal (DAT) having a scanner that is used to scan a financial document, such as a receipt, to create a bitmap image of the document, which can then be compressed. Ex. 1001, 7:52-57, Fig. 2. The specification states that the DAT can use well known encryption algorithms to encrypt the compressed bitmapped image. *Id*. at 7:61-65 and 8:3-10. The specification further discloses that once the ECBI has been generated, a tag is prepended to the ECBI to form the TECBI. *Id*. at 8:13-20; 10:27-57. This process of forming a TECBI is depicted in Fig. 3A, which provides a flowchart of the process with the tag being added after the ECBI has been encrypted.

Patent Owner contends that one skilled in the art would understand that "encrypting subsystem identification information" is directed to encrypting "identification information," such as the transaction data, which is scanned and converted to an ECBI. The claims, however, require encrypting "subsystem identification information" and not merely "identification information."

Based on the record presented, we credit Dr. Alexander's testimony and find that Petitioner has demonstrated that claims 1-41 and 51-69 are more likely than not unpatentable for lack of sufficient written description for encrypting subsystem identification information.

2. *Within and Between*

Petitioner contends that claims 1-123 are unpatentable as the claim term "within and between" lacks sufficient written description. Pet. 48-51. Petitioner states that the '988 patent specification does not describe the transmission of data within subsystems of the same hierarchical level.

Pet. 49. Petitioner cites Dr. Alexander's Declaration for support.

The term "within and between" appears in the Summary of the Invention portion of the '988 patent specification at col. 3, ll. 48-51. We find that Petitioner has failed to demonstrate that claims 1-123 are more likely than not unpatentable for lack of sufficient written description for the term "within and between."

E. Grounds Based on 35 U.S.C. § 101— Claims 1-123 Directed to Non-Statutory Subject Matter

Petitioner contends that claims 1-123 are unpatentable under 35 U.S.C. § 101, because they are directed toward ineligible subject matter. Pet. 21-39. Petitioner relies on the Declaration of Dr. Alexander (Ex. 1003 ¶¶ 104-141) to support its contention that the challenged claims are unpatentably abstract and fail the machine-or-transformation test. *Id*.

Patent Owner asserts that there is nothing "abstract" about encryption of data through the use of software, the transmission of data between locations or subsystems, and the imaging of a document. Prelim. Resp. 27-28. In particular, Patent Owner asserts that the encryption cannot be abstract as there is no mathematical encryption formula disclosed in the '988 patent specification, especially since the '988 patent refers to the use of well-known encryption algorithms. *Id*. Patent Owner further asserts that the claims are directed to a system and that the various system components that might be used in constructing the claimed system are mere examples and "preferred embodiments" rather than absolute requirements. Prelim. Resp. 32-33. Given that the claims are directed to a system, Patent Owner contends that Petitioner has failed to consider the claims as a whole.

On the present record, we determine that Petitioner has shown that claims 1-123 are more likely than not unpatentable under 35 U.S.C. § 101.

The Supreme Court has made it clear that the test for patent eligibility under § 101 is not amenable to bright-line categorical rules. *See Bilski v. Kappos*, 130 S. Ct. 3218 (2010); *see also Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 132 S. Ct. 1289 (2012). Section 101 provides that "[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title." The plain language of the statute and use of the term "any" shows that "Congress contemplated that the patent laws would be given wide scope" for patent eligible subject matter. *Bilski v. Kappos*, 130 S. Ct. 3218, 3225 (2010) (quoting *Diamond v. Chakrabarty*, 447 U.S. 303, 308 (1980)). Accordingly, there are three limited, judicially created exceptions to the broad categories of patent-eligible subject matter in Section 101: laws of nature, natural phenomena, and abstract ideas. *Mayo*, 132 S. Ct. at 1293.

An abstract idea by itself is not patentable, but a practical application of an abstract idea may be deserving of patent protection. *Id*. at 1293-94; *see Bilski*, 130 S. Ct. at 3230; *Diamond v. Diehr*, 450 U.S. 175, 187 (1981). To be patent-eligible, a claim must incorporate enough meaningful limitations to ensure that it claims more than just an abstract idea and is not merely a "drafting effort designed to monopolize the [abstract idea] itself." *Mayo*, 132 S. Ct. at 1297. Limiting the claim to a particular technological environment or field of use, or adding insignificant pre- or post-solution activity, do not constitute meaningful limitations. *See Bilski*, 130 S. Ct. at

3230; *Diehr*, 450 U.S. at 191-92; *Parker v. Flook*, 437 U.S. 584, 595 n.18 (1978).

The subject matter of claims 1-123, when considered as a whole, is directed to an abstract idea; namely the underlying idea of transferring information from one location to another where the transferred information is unreadable without a secret decoder key. Here, the use of private encrypted messages communicated from one location to another represent a "disembodied concept," a basic building block of human ingenuity. Thus, we analyze the claims to determine if they "incorporate enough meaningful limitations to ensure that the claims cover more than just an abstract idea." *See Mayo*, 132 S. Ct. at 1297.

Claim 46 is representative of the challenged claims. Claim 46 is directed to a method comprising capturing an image of documents and receipts and extracting data therefrom, and collecting, managing, encrypting and transmitting the data to various locations within a system. Claim 46 does not require particular apparatus that limit the claim in a meaningful way. Dr. Alexander testifies that the '988 patent simply arranges old well-known elements with each performing the same function it had been known to perform. Patent Owner does not dispute Dr. Alexander's testimony. For example, Patent Owner states that the '988 patent discusses a number of hardware options but that the claims do not claim any "particular" machines or components, as the invention is in the configuration of the system. Prelim. Resp. 32-33. Based on the record presented, we do not see how the limitations in claim 46 are significant meaningful limitations that transform the abstract idea into patent-eligible applications of these abstractions.

Petitioner identifies how the remaining claims, claims 1-45 and 47-123, also add only routine operations and generic computer components to the abstract idea. Patent Owner does not present separate arguments for its claims. Accordingly, based on the record presented, we hold that claims 1-45 and 47-123 do not recite significant meaningful limitations on the abstract idea for the same reasons we held that claim 46 does not recite significant meaningful limitations.

Patent Owner contends that its claims do not preempt any abstract idea, as there is nothing abstract about its claimed system and method claims. We disagree. The claims do not add meaningful limitations to avoid preempting the basic concept of transferring information from one location to another where the transferred information is unreadable without a secret decoder key. Although the claims are limited to capturing images of paper transaction data, to be meaningful, the claim must contain more than mere field-of-use limitations, tangential references to technology, insignificant pre- or post-solution activity, ancillary data-gathering steps, or the like.

Patent Owner also contends that its claims do not fail the machine-or-transformation test in *Bilski*. Prelim. Resp. 32. According to Patent Owner, the particular machine is the claimed system and the claims must be considered as a whole. *Id*. at 33. Patent Owner states that a scanner is used to capture an image of the paper transaction data, and that the system thereafter collects, processes, sends, and stores the data. *Id*. The claims as a whole, however, do not result in any transformed articles. Rather, transaction (financial) data are duplicated, organized, and moved from one place to another. Ex. 1003 ¶¶ 139-141. Further, the fact that the claims involve the use of generic, well-known machines does not impart

patentability under the machine-or-transformation test. *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972) (invalidating as patent-ineligible claimed processes that "can be carried out in existing computers long in use, no new machinery being necessary").

Based on the foregoing, we are persuaded Petitioner has shown that it is more likely than not that claims 1-123 of the '988 patent are directed toward ineligible subject matter under 35 U.S.C. § 101.

III. CONCLUSION

For the foregoing reasons, we are persuaded that the information presented establishes that it is more likely than not that Petitioner would prevail in establishing the unpatentability of claims 1-123 of the '988 patent.

The Board has not made a final determination on the patentability of any challenged claims.

IV. ORDER

Accordingly, it is

ORDERED that pursuant to 35 U.S.C. § 324(a), the Petition for covered business method patent review is *granted* as to claims 1-123 of the '988 patent on the following grounds:

1. Claims 1-123 as being drawn to non-statutory subject matter under 35 U.S.C. § 101; and
2. Claims 1-41 and 51-69 under 35 U.S.C. § 112, 1st paragraph as lacking sufficient written description for encrypting subsystem identification information;

FURTHER ORDERED that pursuant to 35 U.S.C. § 324(d) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial; the trial

commences on the entry date of this decision.

CBM 2014-00021
Patent 5,910,988

For PETITIONER:

Erika H. Arner, Lead Counsel
Darren M. Jiron, Backup Counsel
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.
11955 Freedom Drive
Reston, VA 20190
E-Mail FIS-Ballard@finnegan.com
Telephone 571-203-2700

For PATENT OWNER:

Abraham Hershkovitz, Lead Counsel
Eugene C. Rzucidlo, Backup Counsel
HERSHKOVITZ & ASSOCIATES, PLLC
2845 Duke Street
Alexandria, VA 22314
E-Mail AHershkovitz@Hershkovitz.net
E-Mail GRzucidlo@Hershkovitz.net
Telephone 703-370-4800

US005910988A

United States Patent [19]

Ballard

[11] **Patent Number: 5,910,988**

[45] **Date of Patent: Jun. 8, 1999**

[54] **REMOTE IMAGE CAPTURE WITH CENTRALIZED PROCESSING AND STORAGE**

[75] Inventor: **Claudio R. Ballard**, Lloyd Harbor, N.Y.

[73] Assignee: **CSP Holdings, Inc.**, Lloyd Harbor, N.Y.

[21] Appl. No.: **08/917,761**

[22] Filed: **Aug. 27, 1997**

[51] **Int. Cl.**[6] **H04L 9/00**

[52] **U.S. Cl.** **380/24**

[58] **Field of Search** 380/25, 24

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,201,978	5/1980	Nally	340/146.3
4,264,808	4/1981	Owens et al.	235/379
4,326,258	4/1982	de la Guardia	364/515
4,417,136	11/1983	Rushby et al.	235/379
4,457,015	6/1984	Nally et al.	382/45
4,500,750	2/1985	Elander et al.	380/26
4,523,330	6/1985	Cain	382/7
4,555,617	11/1985	Brooks et al.	235/379
4,578,530	3/1986	Zeidler	380/26
4,602,936	7/1986	Green et al.	382/140
4,680,803	7/1987	Dilella	382/9
4,694,147	9/1987	Amemiya et al.	235/379
4,747,058	5/1988	Ho	364/478
4,750,201	6/1988	Hodgson et al.	379/144
4,843,220	6/1989	Haun	235/380
4,888,812	12/1989	Dinan et al.	382/7
4,912,762	3/1990	Lee et al.	380/24
4,926,325	5/1990	Benton et al.	364/408
4,960,981	10/1990	Benton et al.	235/379
5,091,968	2/1992	Higgins et al.	382/30
5,122,950	6/1992	Benton et al.	364/408
5,144,115	9/1992	Yoshida	235/379
5,159,548	10/1992	Caslavka	364/408
5,173,594	12/1992	McClure	235/380
5,175,682	12/1992	Higashiyama et al.	364/408
5,187,750	2/1993	Behera	382/7
5,204,811	4/1993	Bednar et al.	364/406
5,220,501	6/1993	Lawlor et al.	364/408
5,237,158	8/1993	Kern et al.	235/379
5,274,567	12/1993	Kallin et al.	364/478
5,283,829	2/1994	Anderson	380/24
5,321,238	6/1994	Kamata et al.	235/379
5,321,751	6/1994	Ray et al.	380/23
5,345,090	9/1994	Hludzinski	250/566
5,434,928	7/1995	Wagner et al.	382/187
5,436,970	7/1995	Ray et al.	380/23
5,444,794	8/1995	Uhland, Sr.	382/137
5,457,747	10/1995	Drexler et al.	380/24
5,479,510	12/1995	Olsen et al.	380/24
5,506,691	4/1996	Bednar et al.	358/402
5,544,043	8/1996	Miki et al.	364/406

(List continued on next page.)

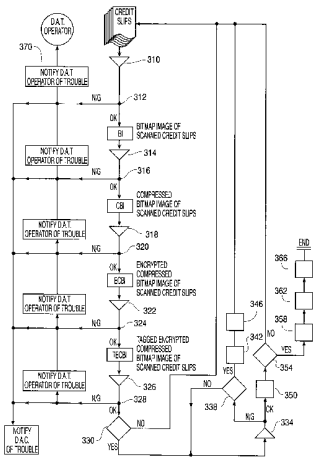
Primary Examiner—Salvatore Cangialosi

Attorney, Agent, or Firm—McGuire, Woods, Battle & Boothe LLP

[57] **ABSTRACT**

A system for remote data acquisition and centralized processing and storage is disclosed called the DataTreasury™ System. The DataTreasury™ System provides comprehensive support for the processing of documents and electronic data associated with different applications including sale, business, banking and general consumer transactions. The system retrieves transaction data at one or more remote Locations, encrypts the data, transmits the encrypted data to a central location, transforms the data to a usable form, performs identification verification using signature data and biometric data, generates informative reports from the data and transmits the informative reports to the remote location (s). The DataTreasury™ System has many advantageous features which work together to provide high performance, security, reliability, fault tolerance and low cost. First, the network architecture facilitates secure communication between the remote location(s) and the central processing facility. A dynamic address assignment algorithm performs load balancing among the system's servers for faster performance and higher utilization. Finally, a partitioning scheme improves the error correction process.

50 Claims, 10 Drawing Sheets



U.S. PATENT DOCUMENTS

5,590,038	12/1996	Pitroda	395/241
5,602,933	2/1997	Blackwell et al.	382/116
5,604,640	2/1997	Zipf et al.	359/803
5,613,001	3/1997	Bakhoum	380/4
5,647,017	7/1997	Smithies et al.	382/119
5,657,389	8/1997	Houvener	380/23
5,657,396	8/1997	Rudolph et al.	382/190
5,673,333	9/1997	Johnston	382/137
5,751,842	5/1998	Riach et al.	382/137
5,754,673	5/1998	Brooks et al.	382/112
5,781,654	7/1998	Carney	382/137
5,784,503	7/1998	Bleecker, III et al.	382/306
5,787,403	7/1998	Randle	705/43

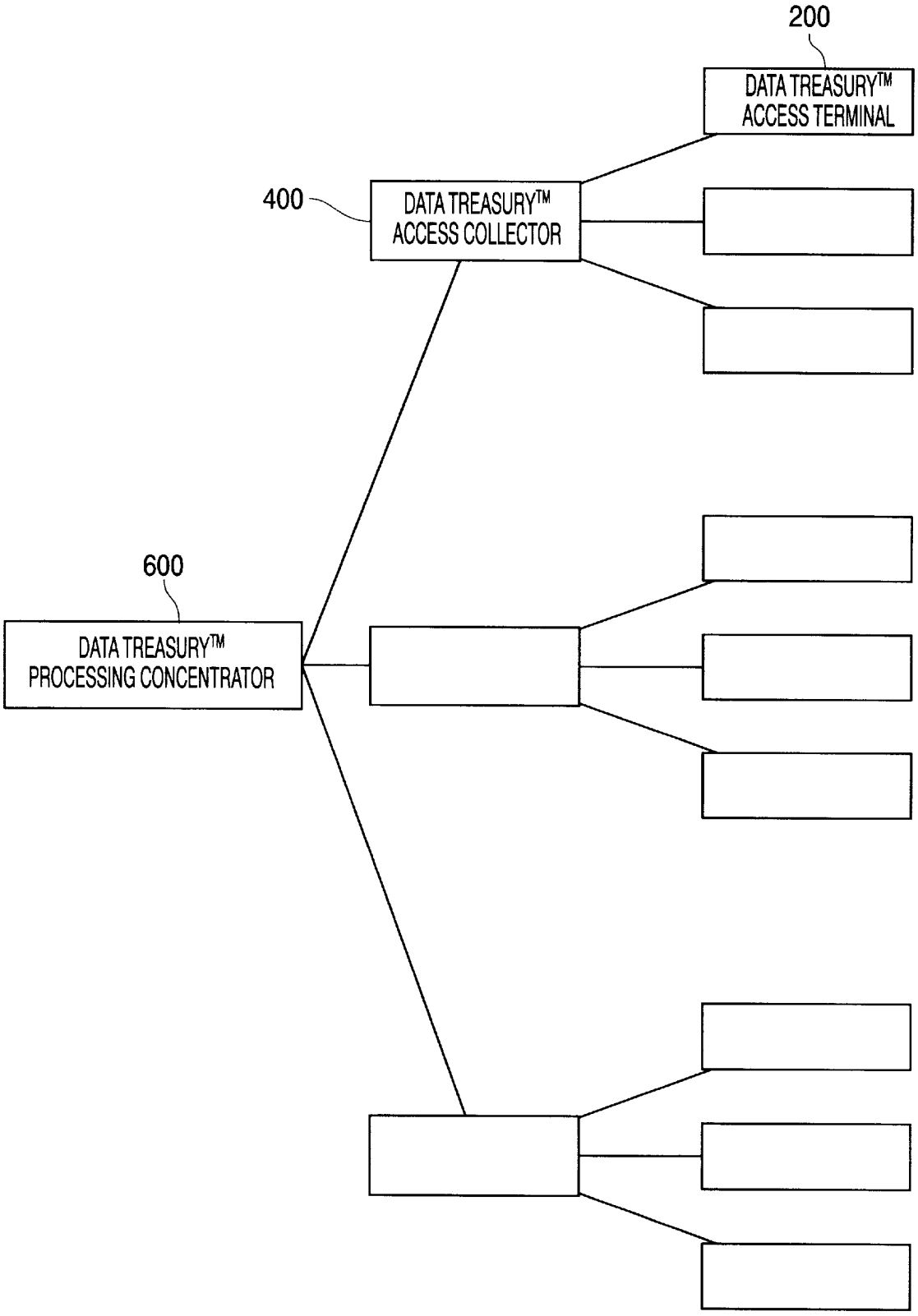

200
DATA TREASURY™ ACCESS TERMINAL
400
DATA TREASURY™ ACCESS COLLECTOR
600
DATA TREASURY™ PROCESSING CONCENTRATOR

FIG. 1

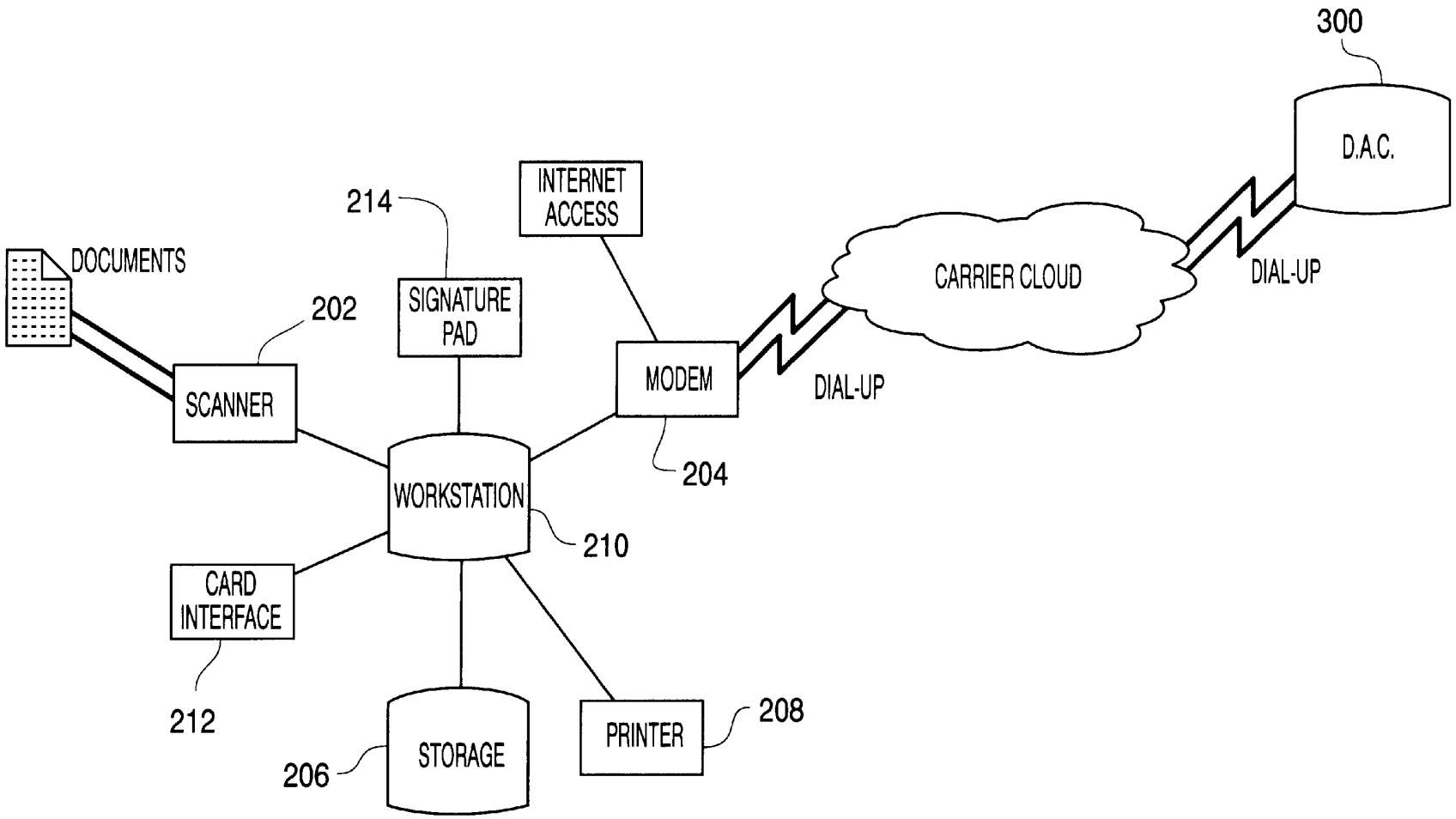

300
D.A.C.
DIAL-UP
CARRIER CLOUD
INTERNET ACCESS
214
SIGNATURE PAD
DOCUMENTS
202
SCANNER
MODEM
DIAL-UP
204
WORKSTATION
210
CARD INTERFACE
212
206
STORAGE
PRINTER
208

FIG. 2

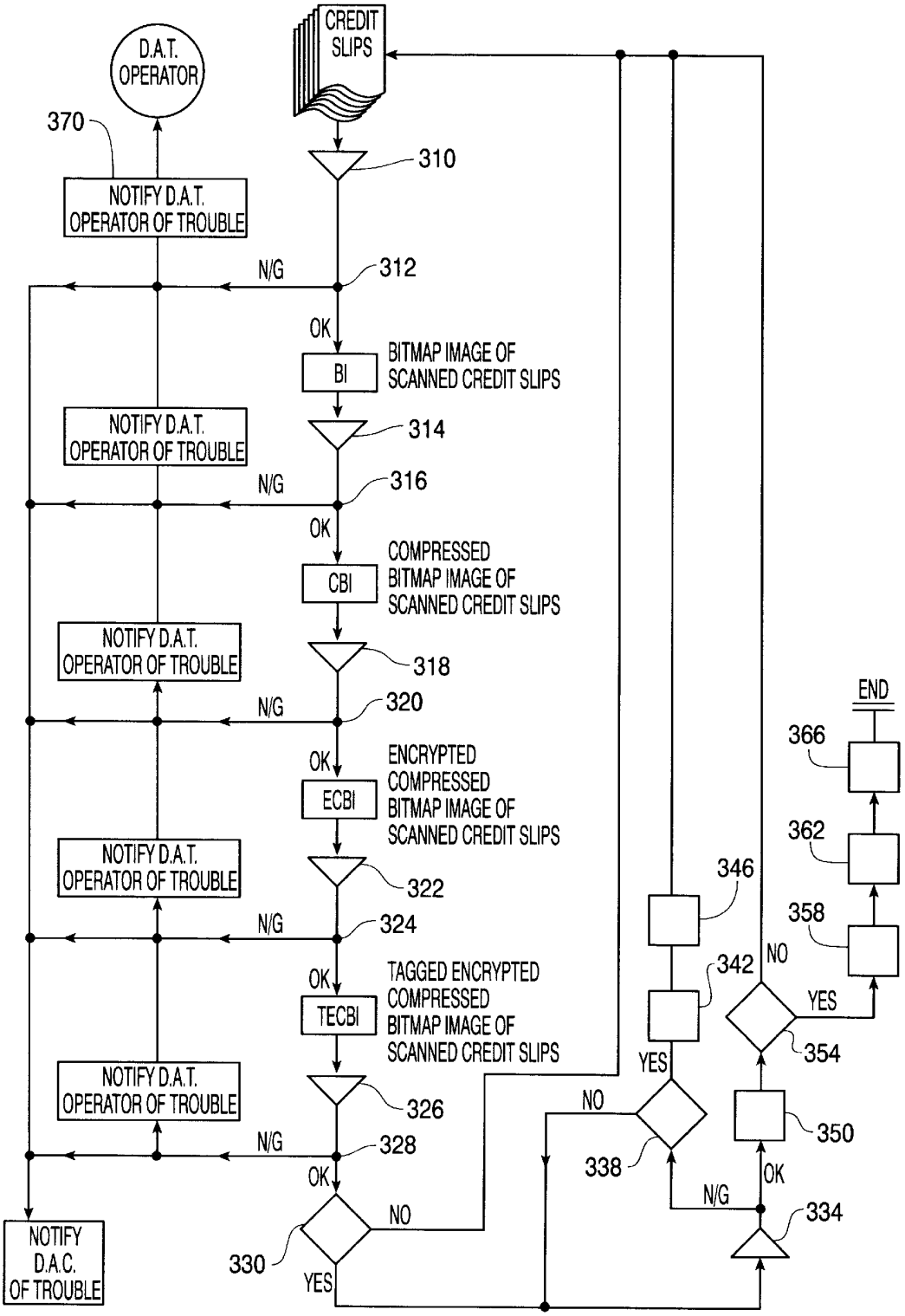

CREDIT SLIPS
D.A.T. OPERATOR
370
310
NOTIFY D.A.T. OPERATOR OF TROUBLE
N/G
312
OK
BI
BITMAP IMAGE OF SCANNED CREDIT SLIPS
NOTIFY D.A.T. OPERATOR OF TROUBLE
314
N/G
316
OK
CBI
COMPRESSED BITMAP IMAGE OF SCANNED CREDIT SLIPS
NOTIFY D.A.T. OPERATOR OF TROUBLE
318
N/G
320
OK
ECBI
ENCRYPTED COMPRESSED BITMAP IMAGE OF SCANNED CREDIT SLIPS
NOTIFY D.A.T. OPERATOR OF TROUBLE
322
N/G
324
OK
TECBI
TAGGED ENCRYPTED COMPRESSED BITMAP IMAGE OF SCANNED CREDIT SLIPS
NOTIFY D.A.T. OPERATOR OF TROUBLE
326
N/G
328
OK
NO
330
YES
NOTIFY D.A.C. OF TROUBLE
346
342
YES
NO
338
N/G
OK
350
334
NO
YES
354
358
362
366
END

FIG. 3A

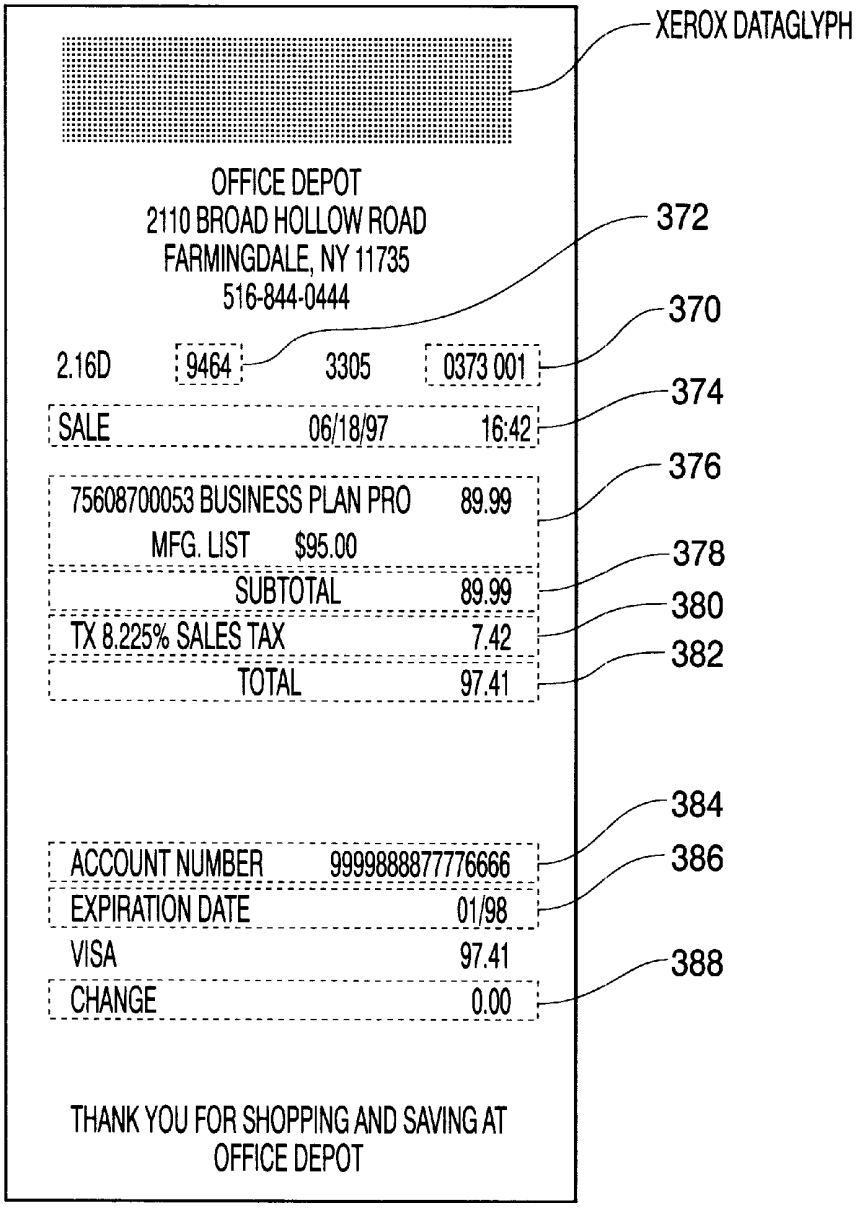

XEROX DATAGLYPH
OFFICE DEPOT
2110 BROAD HOLLOW ROAD
FARMINGDALE, NY 11735
516-844-0444
372
370
2.16D
9464
3305
0373 001
374
SALE
06/18/97
16:42
376
75608700053 BUSINESS PLAN PRO
89.99
MFG. LIST $95.00
378
SUBTOTAL
89.99
380
TX 8.225% SALES TAX
7.42
382
TOTAL
97.41
384
ACCOUNT NUMBER
9999888877776666
386
EXPIRATION DATE
01/98
VISA
97.41
388
CHANGE
0.00
THANK YOU FOR SHOPPING AND SAVING AT
OFFICE DEPOT

FIG. 3B

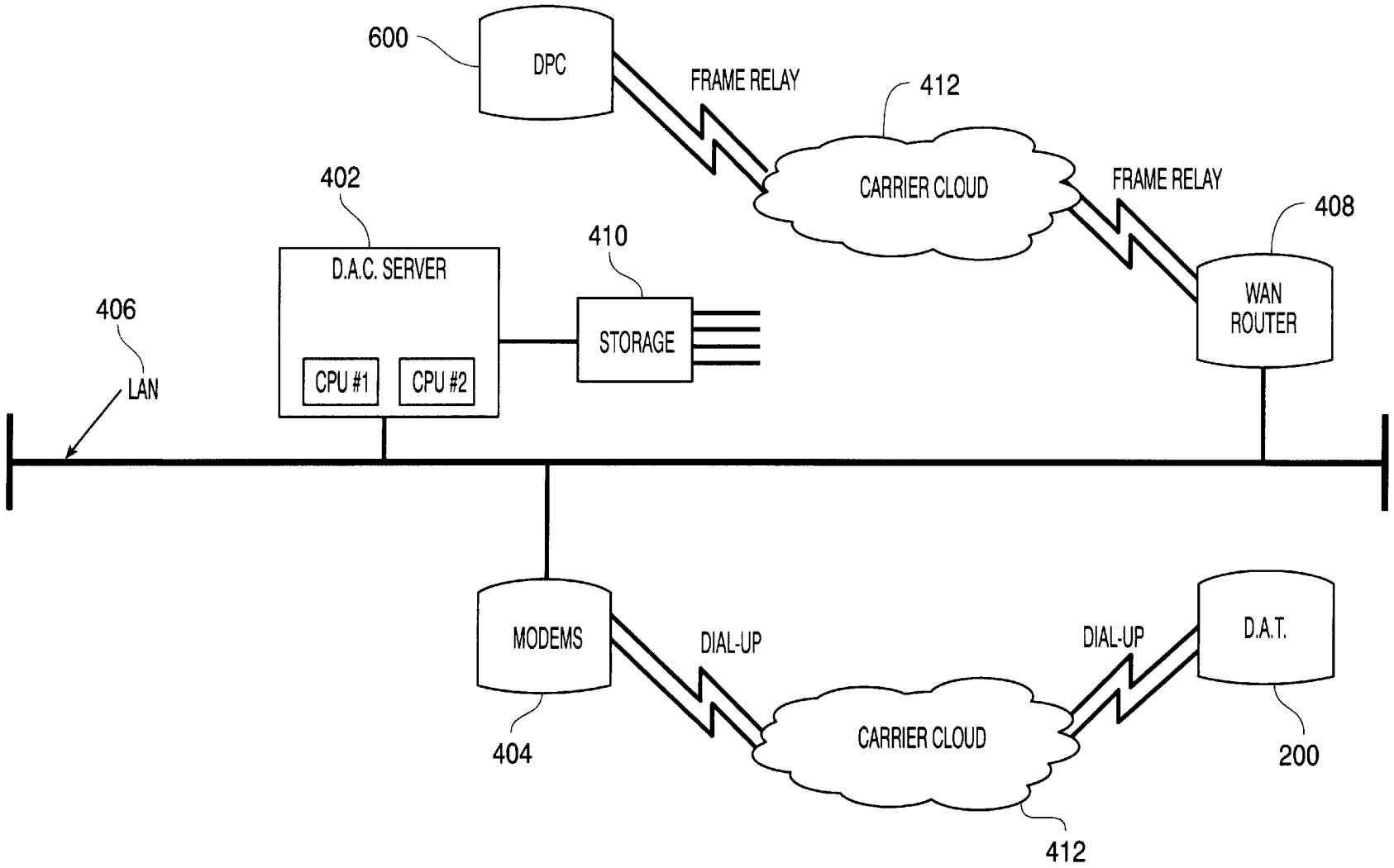

600
DPC
FRAME RELAY
412
CARRIER CLOUD
FRAME RELAY
408
WAN ROUTER
402
D.A.C. SERVER
410
STORAGE
406
LAN
CPU #1
CPU #2
MODEMS
DIAL-UP
DIAL-UP
D.A.T.
CARRIER CLOUD
404
200
412

FIG. 4

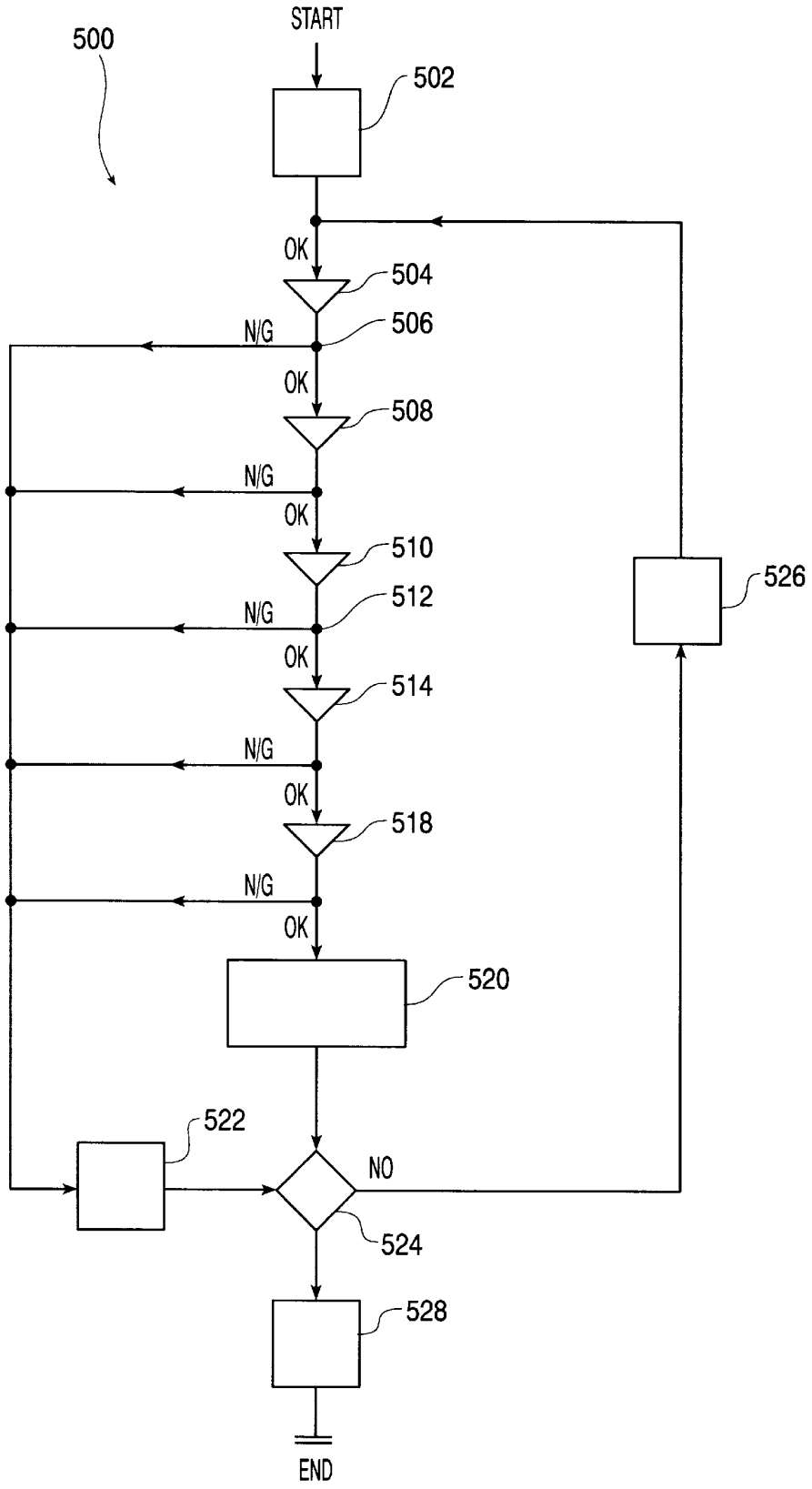

500
START
502
OK
504
N/G
506
OK
508
N/G
OK
510
N/G
512
OK
514
N/G
OK
518
N/G
OK
520
522
NO
524
526
528
END

FIG. 5

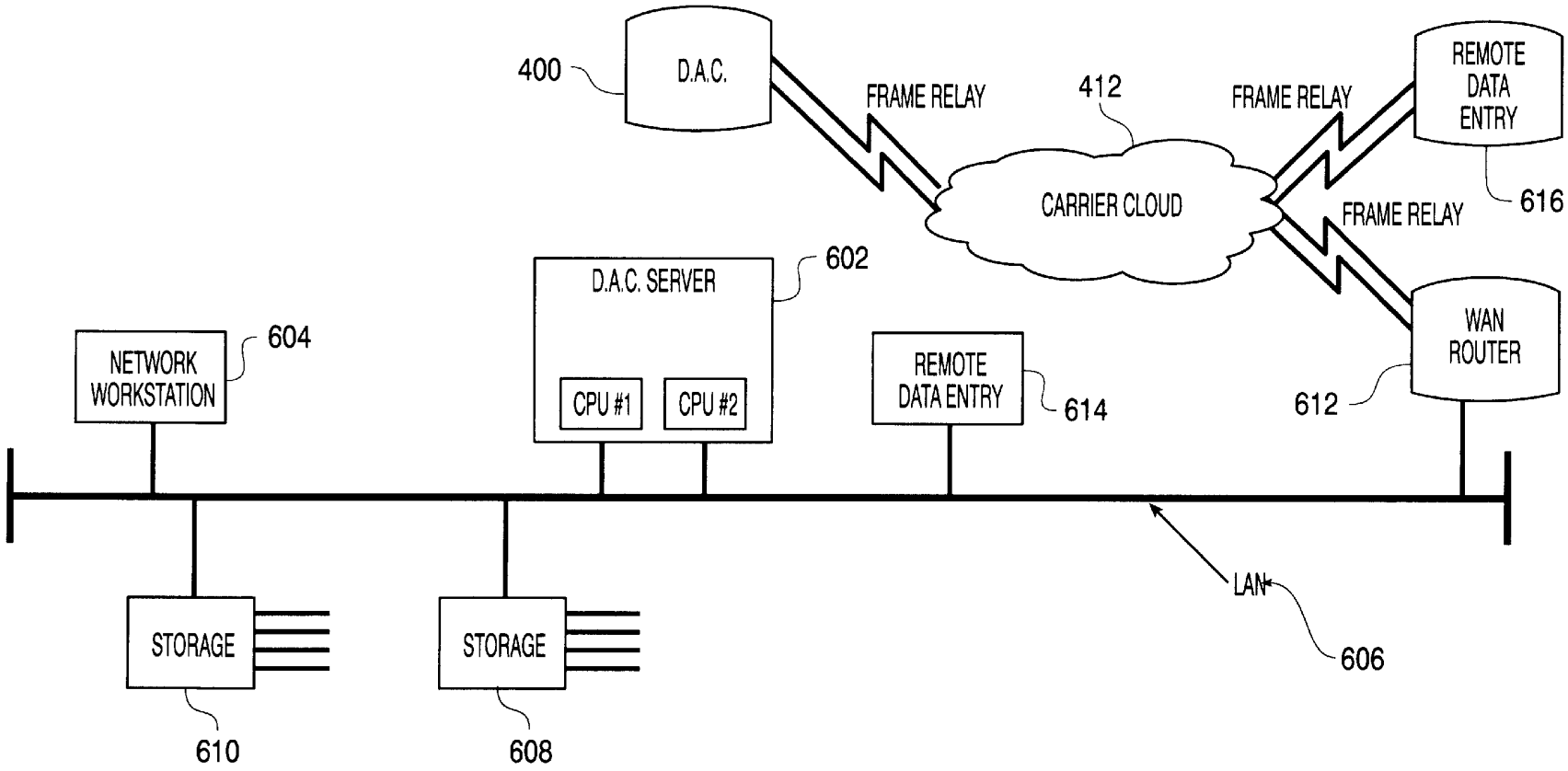

400
D.A.C.
FRAME RELAY
412
FRAME RELAY
REMOTE DATA ENTRY
616
CARRIER CLOUD
FRAME RELAY
602
D.A.C. SERVER
CPU #1
CPU #2
604
NETWORK WORKSTATION
REMOTE DATA ENTRY
614
WAN ROUTER
612
LAN
606
STORAGE
610
STORAGE
608

FIG. 6

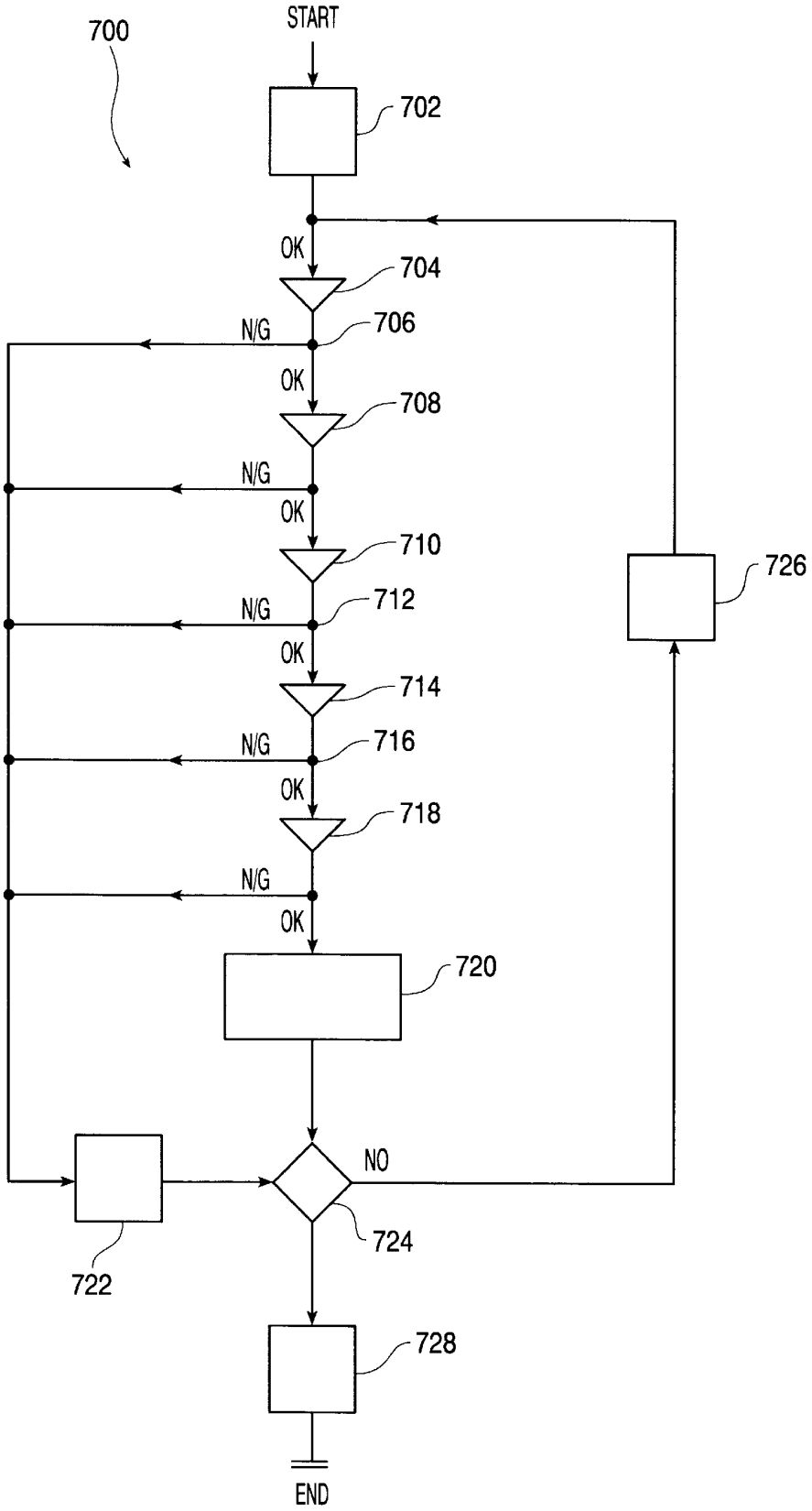

700
START
702
OK
704
N/G
706
OK
708
N/G
OK
710
N/G
712
OK
714
N/G
716
OK
718
N/G
OK
720
726
NO
724
722
728
END

FIG. 7

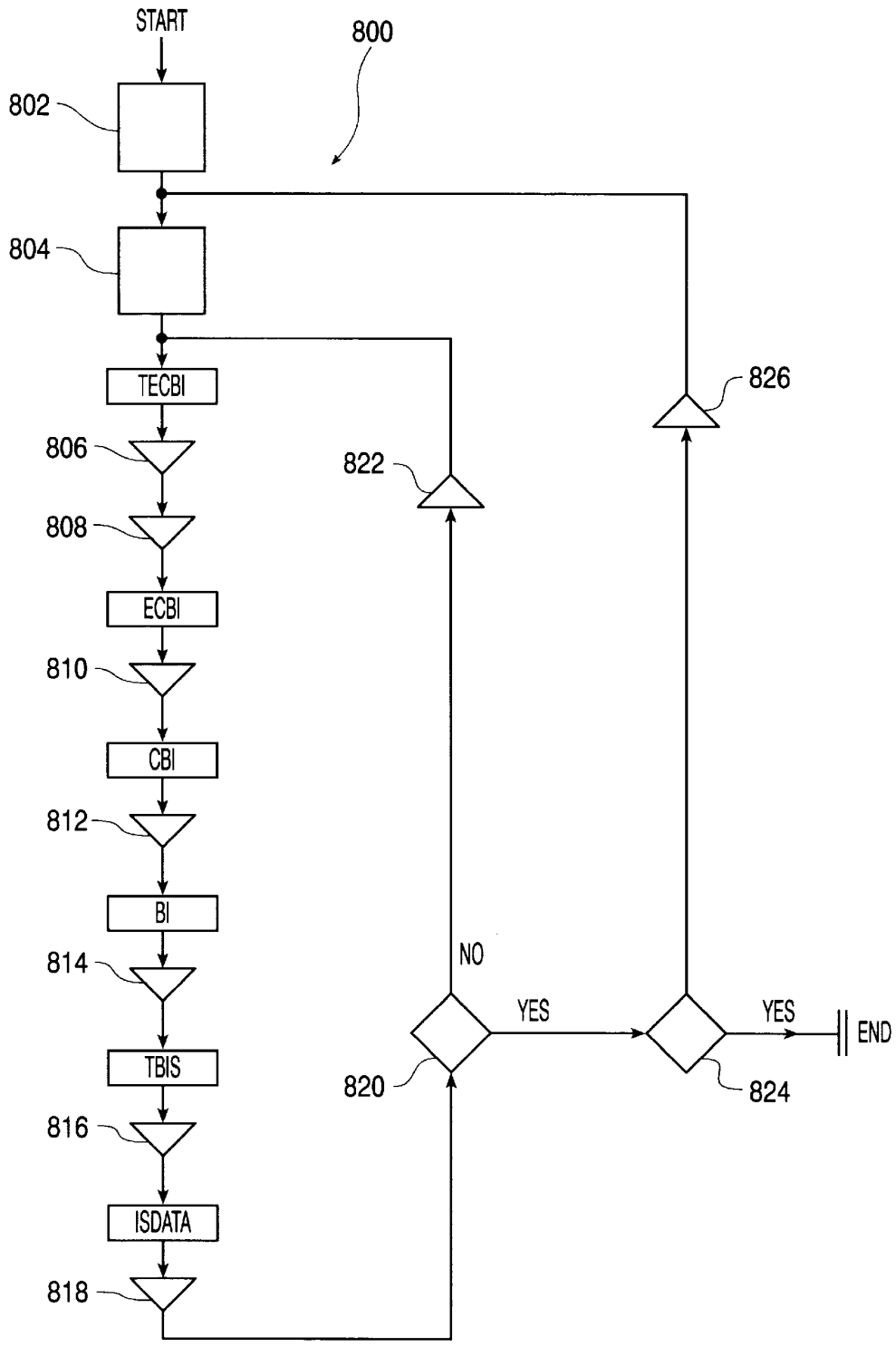

START
800
802
804
TECBI
806
808
ECBI
810
CBI
812
BI
814
TBIS
816
ISDATA
818
822
826
NO
YES
YES
END
820
824

FIG. 8

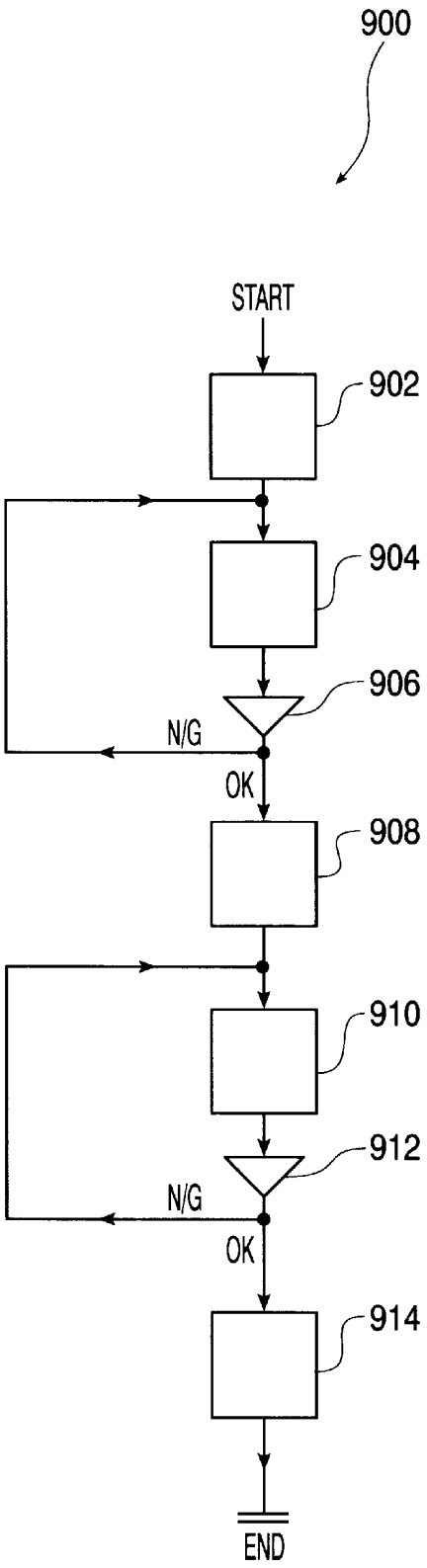


FIG. 9

REMOTE IMAGE CAPTURE WITH CENTRALIZED PROCESSING AND STORAGE

FIELD OF THE INVENTION

This invention relates generally to the automated processing of documents and electronic data from different applications including sale, business, banking and general consumer transactions. More particularly, it pertains to an automated system to retrieve transaction data at remote locations, to encrypt the data, to transmit the encrypted data to a central location, to transform the data to a usable form, to generate informative reports from the data and to transmit the informative reports to the remote locations.

BACKGROUND

This invention involves the processing of documents and electronic data which are generated, for example, from sale, business and banking transactions including credit card transactions, smart card transactions, automated teller machine (ATM) transactions, consumer purchases, business forms, W2 forms, birth certificates, deeds and insurance documents.

The enormous number of paper and electronic records generated from documents and electronic data from sale, business and banking transactions contain valuable information. First, these paper and electronic records contain information which can be used to verify the accuracy of the records maintained by consumers, merchants and bankers. For example, customers use paper receipts of sale and banking transactions to verify the information on the periodic statements which they receive from their bank or credit card institution. Merchants use paper receipts to record sale transactions for management of customer complaints. Taxpayers use paper receipts to record tax deductible contributions for use in their tax return preparation. Employees use paper receipts to record business expenses for preparation of business expense forms.

Paper and electronic records also contain information which can be used for market analysis. For example, manufacturers and retailers can determine consumer preferences in different regions as well as trends in consumer preferences from the information contained in paper and electronic records.

However, the maintenance and processing of paper and electronic records presents difficult challenges. First, paper receipts and documents could easily be lost, misplaced, stolen, damaged or destroyed. Further, the information contained in these paper and electronic records cannot be easily processed because it is scattered among individual records. For example, the market trend information contained in a group of sales records retained by merchants cannot easily be determined since this information is scattered among the individual records. Likewise, the tax information contained in a group of paper receipts of sales transactions retained by consumers cannot easily be processed.

Previous approaches have been proposed to meet the challenges associated with the maintenance and processing of paper and electronic records. For example, data archive service companies store the information from paper receipts and documents acquired from their customers on microfilm or compact disc read only memory (CD-ROM) at a central facility. Customers typically deliver the paper receipts and documents to the central facility. For sensitive documents which cannot leave the customer site, some data archive service companies perform data acquisition and transfer to magnetic tapes at the customer site and deliver the tapes to the central facility.

The approach offered by these data archive service companies have disadvantages. First, the approach is costly and has poor performance because it requires an expensive, time consuming physical transportation of paper receipts or magnetic tapes from the customer site to the central facility. Further, the approach is not reliable as information can be lost or damaged during physical transportation. The approach also has limited capability as it does not process electronic records along with the paper receipts within a single system.

Other approaches have focused on the elimination of paper receipts and documents. U.S. Pat. No. 5,590,038 discloses a universal electronic transaction card (UET card) or smart card which stores transaction information on a memory embedded on the card as a substitute for a paper receipt. Similarly, U.S. Pat. No. 5,479,510 discloses a method of electronically transmitting and storing purchaser information at the time of purchase which is read at a later time to ensure that the purchased goods or services are delivered to the correct person.

While these approaches avoid the problems associated with paper receipts, they have other disadvantages. First, these approaches do not offer independent verification of the accuracy of the records maintained by consumers, merchants and bankers with a third party recipient of the transaction data. For example, if a UET card is lost, stolen, damaged or deliberately altered by an unscrupulous holder after recording sale or banking transactions, these approaches would not be able to verify the remaining records which are maintained by the other parties to the transactions.

Next, these approaches do not have the ability to process both paper and electronic records of transactions within a single, comprehensive system. Accordingly, they do not address the task of processing the enormous number of paper receipts which have been generated from sales and banking transactions. The absence of the ability to process both paper and electronic records of these approaches is a significant limitation as paper receipts and documents will continue to be generated for the foreseeable future because of concerns over the reliability and security of electronic transactions and the familiarity of consumers and merchants with paper receipts.

These approaches also have a security deficiency as they do not offer signature verification which is typically used on credit card purchases to avoid theft and fraud. For example, a thief could misappropriate money from a UET card holder after obtaining by force, manipulation or theft the user's personal identification number (PIN). Similarly, it is not uncommon for criminals to acquire credit cards in victims' names and make unlawful charges after obtaining the victim's social security number. This becomes a greater concern as that type of personal information becomes available, e.g., on the internet. Also, the signature verification performed manually by merchants for credit card purchases frequently misses forged signatures.

Even if smart cards or UET cards had the ability to store signature and other biometric data within the card for verification, the system would still have disadvantages. First, the stored biometric data on the card could be altered by a card thief to defeat the security measure. Similarly, the biometric data could be corrupted if the card is damaged. Finally, the security measure would be costly at it would require an expensive biometric comparison feature either on each card or on equipment at each merchant site.

Additional biometric verification systems including signature verification systems have been proposed to address the security problem. For example, U.S. Pat. No. 5,657,393 discloses a method and apparatus for verification of handwritten signatures involving the extraction and comparison of signature characteristics including the length and angle of select component lines. In addition, U.S. Pat. No. 5,602,933 discloses a method and apparatus for the verification of remotely acquired data with corresponding data stored at a central facility.

However, none of these verification systems offer general support for transaction initiation, remote paper and electronic data acquisition, data encryption, data communication, data archival, data retrieval, data mining, manipulation and analytic services. Accordingly, there is a need for a single system which offers comprehensive support for the tasks involved in the automated processing of documents, biometric and electronic data from sale, business, banking and general consumer transactions. Further, there is a need for a single comprehensive system having the reliability, performance, fault tolerance, capacity, cost and security to satisfy the requirements of the retail, business, banking and general consumer industries.

SUMMARY OF THE INVENTION

The invention provides an automated, reliable, high performance, fault tolerant, and low cost system with maximal security and availability to process electronic and paper transactions, and has been named the DataTreasury™ System.

It is an object of the present invention to provide a system for central management, storage and verification of remotely captured electronic and paper transactions from credit cards, smart cards, debit cards, documents and receipts involving sales, business, banking and general purpose consumer applications comprising:

- at least one remote data access subsystem for capturing and sending electronic and paper transaction data;
- at least one data collecting subsystem for collecting and sending the electronic and paper transaction data comprising a first data management subsystem for managing the collecting and sending of the transaction data;
- at least one central data processing subsystem for processing, sending and storing the electronic and paper transaction data comprising a second data management subsystem for managing the processing, sending and storing of the transaction data; and
- at least one communication network for the transmission of the transaction data within and between said at least one data access subsystem and said at least one data processing subsystem.

The DataTreasury™ System processes paper and/or electronic receipts such as credit card receipts, Automated Teller Machine (ATM) receipts, business expense receipts and sales receipts and automatically generates reports such as credit card statements, bank statements, tax reports for tax return preparation, market analyses, and the like.

It is a further object of the DataTreasury™ System to retrieve both paper and electronic transactions at remote locations.

It is a further object of the DataTreasury™ System to employ a scanner and a data entry terminal at a customer site to retrieve data from paper transactions and to enable additions or modifications to the scanned information respectively.

It is a further object of the DataTreasury™ System to provide an input device for retrieving transaction data from the memory of smart cards for independent verification of the records maintained by consumers, merchants and bankers to prevent the loss of data from the loss, theft, damage or deliberate alteration of the smart card.

It is a further object of the DataTreasury™ System to retrieve and process transaction data from DataTreasury™ System anonymous smart cards which are identified by an account number and password. Since DataTreasury™ System anonymous smart card transactions can be identified without the customer's name, a customer can add money to the DataTreasury™ System anonymous smart card and make expenditures with the card with the same degree of privacy as cash acquisitions and expenditures.

It is a further object of the DataTreasury™ System to retrieve customer billing data from employee time documents and to generate customer billing statements from the billing data.

It is a further object of the DataTreasury™ System to initiate electronic transactions including transactions on the internet and to provide identification verification by capturing and comparing signature and biometric data.

It is a further object of the DataTreasury™ System of the invention to process electronic and paper transactions with a tiered architecture comprised of DataTreasury™ System Access Terminals (DATs), DataTreasury™ System Access Collectors (DACS) and DataTreasury™ System Processing Concentrators (DPCs).

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects and features of the invention will be more clearly understood from the following detailed description along with the accompanying drawing figures, wherein:

FIG. **1** is a block diagram showing the three major operational elements of the invention: the DataTreasury™ System Access Terminal (DAT), the DataTreasury™ System Access Collector (DAC) and the DataTreasury™ System Processing Concentrator (DPC);

FIG. **2** is a block diagram of the DAT architecture;

FIG. **3***a* is a flow chart describing image capture by a DAT;

FIG. **3***b* displays a sample paper receipt which is processed by the DAT;

FIG. **4** is a block diagram of the DAC architecture;

FIG. **5** is a flow chart describing the polling of the DATs by a DAC;

FIG. **6** is a block diagram of the DPC architecture;

FIG. **7** is a flow chart describing the polling of the DACs by the DPC;

FIG. **8** is a flow chart describing the data processing performed by the DPC; and

FIG. **9** is a flow chart describing the data retrieval performed by the DPC.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. **1** shows the architecture of the DataTreasury™ System **100**. The DataTreasury™ System **100** has three operational elements: the DataTreasury™ System Access Terminal (DAT) **200** (the remote data access subsystem), the DataTreasury™ System Access Collector (DAC) **400** (the intermediate data collecting subsystem), and the DataTreasury™ System Processing Concentrator (DPC) **600** (the central data processing subsystem).

The DataTreasury™ System **100** architecture consists of three tiers. At the bottom tier, the DATs **200** retrieve data from the customer sites. At the next tier, the DACs **400** poll the DATs **200** to receive data which accumulates in the DATs **200**. At the top tier, the DPCs **600** poll the DACs **400** to receive data which accumulates in the DACs **400**. The DPCs **600** store the customer's data in a central location, generate informative reports from the data and transmit the informative reports to the customers at remote locations.

In the preferred embodiment, the DataTreasury™ System **100** complies with the Price Waterhouse SAS70 industry standard. Specifically, the DataTreasury™ System **100** meets the software development standard, the system deployment standard and the reliability standard specified by Price Waterhouse SAS70. By adhering to the Price Waterhouse SAS70 standard, the DataTreasury™ System **100** provides the security, availability and reliability required by mission critical financial applications of banks and stock brokerage companies.

As is known to persons of ordinary skill in the art, the DataTreasury™ System **100** could also use other software development standard, other system deployment standards and other reliability standards as long as adherence to these alternative standards provides the security, availability and reliability required by mission critical financial applications.

FIG. **2** shows a block diagram of the DAT **200** architecture. DATs **200** are located at customer sites. The DataTreasury™ System **100** customers include merchants, consumers and bankers. The DATs **200** act as the customer contact point to the suite of services provided by the DataTreasury™ System **100**. In the preferred embodiment, the DAT **200** is custom designed around a general purpose thin client Network Computer (NC) which runs SUN Microsystem's JAVA/OS operating system. The custom designed DAT **200** comprises a DAT scanner **202**, a DAT modem **204**, DAT digital storage **206**, a DAT controller **210** (workstation), a DAT card interface **212**, an optional DAT printer **208** and a signature pad **214**.

As is known to persons of ordinary skill in the art, the DAT **200** could also be custom designed around a general purpose network computer running other operating systems as long as the chosen operating system provides support for multiprocessing, memory management and dynamic linking required by the DataTreasury™ System **100**.

The DAT scanner **202** scans a paper receipt and generates a digital bitmap image representation called a Bitmap Image (BI) of the receipt. In the preferred embodiment, the DAT scanner **202** has the ability to support a full range of image resolution values which are commonly measured in Dots Per Inch (DPI). Next, the DAT scanner **202** has the ability to perform full duplex imaging. With full duplex imaging, a scanner simultaneous captures both the front and back of a paper document. The DAT scanner **202** can also support gray scale and full color imaging at any bit per pixel depth value. The DAT scanner **202** also supports the capture of handwritten signatures for identity verification.

In addition to scanning images and text, the DAT scanner **202** also scans DataGlyph™ elements, available from Xerox Corporation. As is known to persons of ordinary skill in the art, the Xerox DataGlyph™ Technology represents digital information with machine readable data which is encoded into many, tiny, individual glyph elements. Each glyph element consists of a 45 degree diagonal line which could be as short as 1/100th of an inch depending on the resolution of the scanning and printing devices. Each glyph element represents a binary 0 or 1 depending on whether it slopes downward to the left or the right respectively. Accordingly, DataGlyph™ elements can represent character strings as ASCII or EBCIDIC binary representations. Further, encryption methods, as known to persons of ordinary skill in the art encrypt the data represented by the DataGlyph™ Technology.

The use of glyph technology in the DataTreasury™ System **100** improves the accuracy, cost and performance of the system. Xerox DataGlyph™ Technology includes error correction codes which can be referenced to correct scanning errors or to correct damage to the document caused by ink spills or ordinary wear. DataGlyph™ Technology also leads to decreased system cost since the system will require less manual intervention for data entry and correction because of the improved accuracy associated with DataGlyph™ elements. Since DataGlyph™ elements represent a large amount of information in a small amount of space, the DAT scanner **100** will require a small amount of time to input a large amount of information.

The DAT card interface **212** and the DAT signature pad **214** along with the internet and telephone access through the DAT modem **204** enable the DataTreasury™ System **100** customer to initiate secure sale and banking transactions via the internet or telephone with the DAT **200** using a variety of cards including debit cards, smart cards and credit cards. After selecting a purchase or a banking transaction through a standard internet interface, the DataTreasury™ System **100** customer inserts or swipes the debit card, smart card or credit card into the DAT card interface **212**.

The DAT card interface **212** retrieves the identification information from the card for subsequent transmission to the destination of the internet transaction. Further, the DAT scanner **202** could capture a hand written signature from a document or the DAT signature pad **214** could capture an electronic signature written on it with a special pen. Similarly, these security featurs allow a credit card recipient to activate the card with a DAT **200** located at a merchant site. The security features would detect unauthorized use of debit cards, credit cards and smart cards resulting from their unlawful interception. Accordingly, the DataTreasury™ System's **100** security features offer a more secure alternative for internet and telephone transactions than the typical methods which only require transmission of a card account number and expiration date.

As is known to persons of ordinary skill in the art, the DATs **200** could also include additional devices for capturing other biometric data for additional security. These devices include facial scans, fingerprints, voice prints, iris scans, retina scans and hand geometry.

In addition to initiating sale and banking transactions, the DAT card interface **212** also reads sale and banking transactions initiated elsewhere from the memory of smart cards to enable subsequent storage and processing by the DataTreasury™ System. If a smart card is lost, stolen, damaged or deliberately altered by an unscrupulous holder after the DAT card interface **212** reads its transaction data, the DataTreasury™ System **100** can reproduce the transaction data for the customer. Accordingly, the DAT card interface **212** provides support for independent verification of the records maintained by consumers, merchants and bankers to prevent the loss of data from the loss, theft, damage or deliberate alteration of the smart card.

The DAT card interface **212** also supports the initiation and retrieval of sale and banking transactions with the DataTreasury™ System anonymous smart cards. In contrast to standard debit cards and credit cards, the DataTreasury™

System anonymous smart card does not identify the card's holder by name. Instead, the DataTreasury™ System anonymous smart card requires only an account number and a password. Since DataTreasury™ system anonymous smart card transactions can be identified without the customer's name, a DataTreasury™ System **100** customer can purchase a DataTreasury™ System anonymous smart card, add money to the card, make expenditures with the card and monitor the card's account with the same degree of privacy as cash acquisition, expenditure and management.

The DAT scanner **202**, the internet access, the signature pad **214** and other biometric data capture devices also support the remote capture of survey information and purchase orders. For example, the DAT scanner **202** captures surveys appearing on the back of checks at restaurants and bars. Similarly, the DAT scanner **202** could capture purchase orders from residences, enabling customers to make immediate purchases from their home of goods promoted through the mail. Accordingly, home marketing merchant could transmit sales in a more cost efficient and reliable manner by using the DAT scanner **202** instead of providing envelopes with prepaid postage to residences.

The DAT scanner **202** also captures receipts which are subsequently needed for tax return preparation or tax audits. Similarly, the DAT scanner **202** captures sales receipts from merchants, providing an off-site secure, reliable repository to guard against loss resulting from flooding, fire or other circumstances. This feature could also allow a merchant to automatically perform inventory in a reliable and cost-effective manner.

The DAT controller **210** performs processing tasks and Input/Output (I/O) tasks which are typically performed by a processor. The DAT controller **210** compresses, encrypts and tags the BI to form a Tagged Encrypted Compressed Bitmap Image (TECBI). The DAT controller **210** also manages the Input/Output (I/O). Specifically, the DAT controller **210** manages devices like the DAT scanner **202**, the DAT digital storage **206**, the optional DAT printer **208** and the DAT modem **204**.

The DAT digital storage **208** holds data such as the TECBI. The DAT modem **204** transmits data from the DAT **200** to the appropriate DAC **400** as instructed by the DAT controller **210**. Specifically, the DAT modem **204** transmits the TECBIs from the DAT digital storage **208** to the appropriate DAC **400**. In the preferred embodiment, the DAT modem **204** is a high speed modem with dial-up connectivity. The DAT digital storage **208** is sufficiently large to store the input data before transmission to a DAC **400**. The DAT digital storage **208** can be Random Access Memory (RAM) or a hard drive.

FIG. **3***a* is a flow chart **300** describing the operation of the DAT in detail. In step **310**, the DAT scanner **202** scans paper receipts into the DAT **200** provided by an operator. In step **312**, the DAT controller **210** determines whether the operation executed successfully. If the scanning is successful, the DAT scanner **202** produces a Bitmap Image (BI). If the scanning is unsuccessful, the DAT controller **210** notifies the operator of the trouble and prompts the operator for repair in step **370**.

If a BI is created, the DAT controller **210** executes a conventional image compression algorithm like the Tagged Image File Format (TIFF) program to compress the BI in step **314**. In step **316**, the DAT controller **210** determines whether the compression executed successfully. If the compression is successful, it produces a Compressed Bitmap Image (CBI). If the compression is unsuccessful, the DAT controller **210** notifies the operator of the trouble and prompts the operator for repair in step **370**.

If a CBI is created, the DAT controller **210** executes an encryption algorithm which is well known to an artisan of ordinary skill in the field to encrypt the CBI in step **318**. Encryption protects against unauthorized access during the subsequent transmission of the data which will be discussed below. In step **320**, the DAT controller **210** determines whether the encryption operation executed successfully. If the encryption is successful, it produces an Encrypted Compressed Bitmap Image (ECBI). If the encryption is unsuccessful, the DAT controller **210** notifies the operator of the trouble and prompts the operator for repair in step **370**.

If an ECBI is created, the DAT controller **210** tags the ECBI with a time stamp which includes the scanning time, an identification number to identify the merchant originating the scan and any additional useful information in step **322**. In step **324**, the DAT controller **210** determines whether the tagging operation executed successfully. If the tagging is successful, it produces a Tagged Encrypted Compressed Bitmap Image (TECBI). If the tagging is unsuccessful, the DAT controller **210** notifies the operator of the trouble and prompts the operator for repair in step **370**.

If a TECBI is created, the DAT controller **210** stores the TECBI in the DAT digital storage **208** in step **326**. In step **328**, the DAT controller **210** determines whether the storing operation executed successfully. If the storing operation is successful, the DAT digital storage **208** will contain the TECBI. If the storing operation is unsuccessful, the DAT controller **210** notifies the operator of the trouble and prompts the operator for repair in step **370**.

If the TECBI is properly stored in the DAT digital storage **208**, the DAT controller **210** determines whether all paper receipts have been scanned in step **330**. If all paper receipts have not been scanned, control returns to step **310** where the next paper receipt will be processed as discussed above. If all paper receipts have been scanned, the DAT controller **210** asks the operator to verify the number of scanned receipts in step **334**. If the number of scanned receipts as determined by the DAT controller **210** does not equal the number of scanned receipts as determined by the operator, the DAT controller **210** asks whether the operator desires to rescan all of the receipts in step **338**.

If the operator chooses to rescan all of the receipts in step **338**, the DAT controller **210** will delete all of the TECBIs associated with the batch from the DAT digital storage **208** in step **342**. After the operator prepares the batch of receipts for rescan in step **346**, control returns to step **310** where the first receipt in the batch will be processed as discussed above.

If the operator chooses not to rescan all of the receipts from the batch in step **338**, control returns to step **334** where the DAT controller **210** asks the operator to verify the number of scanned receipts as discussed above.

If the number of scanned receipts as determined by the DAT controller **210** equals the number of scanned receipts as determined by the operator, the DAT controller **210** prints a batch ticket on the DAT printer **206** in step **350**. The operator will attach this batch ticket to the batch of receipts which have been scanned. This batch ticket shall contain relevant session information such as scan time, number of receipts and an identification number for the data operator. If processing difficulties occur for a batch of receipts after the image capture of flowchart **300**, the batch ticket will enable them to be quickly located for rescanning with the DAT **200**.

In step **354**, the DAT controller **210** determines whether the scan session has completed. If the scan session has not

completed, control returns to step **310** where the first receipt in the next batch of the scan session will be processed as discussed above. If the scan session has completed, the DAT controller **210** selectively prints a session report on the DAT printer **206** in step **358**. The DAT controller **210** writes statistical information for the session to the DAT digital storage **208** in step **362**. In step **366**, the DAT controller **210** terminates the session.

FIG. **3***b* displays a sample paper receipt which is processed by the DAT **200** as described by the flowchart in FIG. **3***a*. The sample paper receipt involves a credit card transaction which has four participants:

A. The ISSUER: is an entity such as a bank or corporate financial institution such as GE Capital, GM or AT&T which provides the credit behind the credit card and issues the card to the consumer.

B. The PROCESSOR: executes the processing of an inbound credit card transaction by performing basic transaction validation that includes checking with the ISSUER database to ensure that the credit card has sufficient credit to allow approval of the transaction.

C. The ACOUIRER: specializes in the marketing, installation and support of Point Of Sale (POS) credit card terminals. The acquirer, like the DAC **400** in the DataTreasury™ System **100** acts as an electronic collection point for the initial credit card transaction as the card is inserted into the POS terminal. After acquisition, the acquirer passes the transaction to the PROCESSOR.

D. The MERCHANT: inserts a credit card into a POS terminal and enters the amount of the transaction to initiate the credit card transaction.

In the preferred embodiment, the DAT **200** reads the following information from the sample paper receipt shown in FIG. **3**i band stores the information in the format described below.

CUSTOMER_ID **370**: This field is a 7 position HEX numeric value. This field uniquely identifies the customer using the terminal. In this sample, this field would identify the credit card merchant.

TERMINAL_ID **372**: This field is a 6 position decimal numeric value. This field uniquely identifies the credit card terminal which is used to print the credit card receipt.

TRANSACTION_DATE **374**: This field contains the date and time of the credit card transaction.

TRANSACTION_LINE_ITEM **376**: This field is a variable length character string. The first three positions represent a right justified numeric field with leading zeros indicating the full length of this field. This field contains all data pertaining to the purchased item including the item's price. The DAT **200** will store a TRANSACTION_LINE_ITEM field for each transaction line item on the receipt. This field is optional since not all credit card transactions will have line items.

TRANSACTION_SUBTOTAL **378**: This field is a double precision floating point number. This field indicates the subtotal of the TRANSACTION_LINE_ITEMs.

TRANSACTION_SALES_TAX **380**: This field is a double precision floating point number. This field contains the sales tax of the TRANSACTION_SUBTOTAL.

TRANSACTION_AMOUNT **382**: This field is a double precision floating point number. This field is the sum of the TRANSACTION_SUBTOTAL and TRANSACTION_SALES_TAX.

CREDIT_CARD_ACCT_NUM **384**: This field is a 12 position decimal value. This field identifies the credit card which was used to execute this transaction.

CREDIT_CARD_EXP_DATE **386**: This field identifies the expiration date of the credit card.

TRANSACTION_APPROVAL_CODE **388**: This field is a 6 position numeric value. This field indicates the approval code that was given for the particular transaction.

The DAT **200** also stores additional items which are not pictured in FIG. **3***b* as described below:

ISSUER_ID: This field is a 7 position decimal numeric value. This field identifies the credit card issuer.

ACQUIRER_ID: This field is a 7 position decimal numeric value. This field identifies the acquirer.

PROCESSOR_ID: This field is a 7 position decimal numeric value. This field identifies the processor.

TRANSACTION_LINE_ITEM_CNT: This field is a 3 position decimal numeric value. This field identifies the number of transaction line items on the receipt. A value of ZERO indicates the absence of any transaction line items on the receipt.

TRANSACTION_GRATUITY: This field is a double precision floating number. This field is optional because it will only appear on restaurant or bar receipts.

FINAL_TRANSACTION_AMOUNT: This field is a double precision floating number. This field is optional because it will only appear on restaurant and bar receipts. The field is the sum of the TRANSACTION_AMOUNT and TRANSACTION_GRATUITY.

The tag prepended to the ECBI in step **322** of the flowchart of FIG. **3***a* identifies the time and place of the document's origination. Specifically, the tag consists of the following fields:

DAT_TERMINAL_ID: This field is a 7 position hexadecimal numeric value. This field uniquely identifies the DAT **200** which is used by the customer.

DAT_SESSION_DATE: This field identifies the date and time of the DAT **200** session which generated the image of the document.

DAT_USER_ID: This field is a 4 position decimal numeric value. This field identifies the individual within the CUSTOMER's organization who initiated the DAT **200** session.

DATA_GLYPH_RESULT: This field is a variable length character string. The first four positions hold a right justified numeric position with leading zero which indicate the length of the field. The fifth position indicates the DataGlyph™ element status. A value of 0 indicates that the data glyph was NOT PRESENT on the receipt. A value of 1 indicates that the data glyph WAS PRESENT and contained no errors. A value of 2 indicates that the data glyph WAS PRESENT and had nominal errors. If the fifth position of this field has a value of 2, the remaining portion of the string identifies the erroneous field numbers. As subsequently described, the DPC **600** will reference this portion of the field to capture the erroneous data from the receipt with alternate methods. A value of 3 indicates that the data glyph WAS PRESENT WITH SEVERE ERRORS. In other words, a value of 3 indicates the DataGlyph™ element was badly damaged and unreadable.

The receipt shown in FIG. **3***b* can also contain a signature which can be captured by the DAT scanner **202**. A data glyph could identify the location of the signature on the receipt.

As is known to persons of ordinary skill in the art, the DataTreasury™ System **100** can also process receipts with alternate formats as long as the receipt contains the appropriate identification information such as the transaction amount, the customer, the DAT **200**, the transaction date, the transaction tax, the credit card number, the credit card expiration date, etc.

The DataTreasury™ System **100** partitions the paper receipt into image snippets as illustrated by the sample on FIG. **3***b*. Partitioning facilitates an improvement in the process to correct errors from the scanning operation. If an error occurred during scanning, the DataTreasury™ System **100** corrects the error using manual entry. With partitioning, the DataTreasury™ System **100** focuses the correction effort on only the image snippet having the error instead of correcting the entire document. The subsequently discussed schema of the DataTreasury™ System **100** database describes the implementation of the partitioning concept in detail.

The DACs **400** form the backbone of the tiered architecture shown in FIG. **1** and FIG. **4**. As shown in FIG. **1**, each DAC **400** supports a region containing a group of DATs **200**. Each DAC **400** polls the DATs **200** in its region and receives TECBIs which have accumulated in the DATs **200**. The DACs **400** are located at key central sites of maximum merchant density.

In the preferred embodiment, the DAC server **402** comprises stand-alone Digital Equipment Corporation (DEC) SMP Alpha 4100 2/566 servers which are connected on a common network running Windows NT. The DEC Alpha servers manage the collection and intermediate storage of images and data which are received from the DATs **200**.

As is known to persons of ordinary skill in the art, the DataTreasury™ System **100** could use any one of a number of different servers that are available from other computer vendors as long as the server meets the capacity, performance and reliability requirements of the system.

In the preferred embodiment, the DAC server **402** also comprises EMC **3300** SYMMETRIX CUBE Disk Storage Systems, which store the images and data collected and managed by the DEC Alpha servers. The DAC **400** architecture also uses a SYMMETRIX Remote Data Facility (SRDF), available from EMC, to enable multiple, physically separate data centers housing EMC Storage Systems to maintain redundant backups of each other across a Wide Area Network (WAN). Since SRDF performs the backup operations in the background, it does not affect the operational performance of the DataTreasury™ System **100**. The DAC server **402** also has secondary memory **410**. In the preferred embodiment, the secondary memory **410** is a small scale DLT jukebox.

The DAC Alpha servers of the DAC server **402** insert images and data received from the DATS **200** into a database which is stored on the disk storage systems using a data manipulation language as is well known to persons of ordinary skill in the art. In the preferred embodiment, the database is a relational database available from Oracle.

As is well known to persons of ordinary skill in the art, the DataTreasury™ System **100** could use any one of a number of different database models which are available from other vendors including the entity relationship model as long as the selected database meets the storage and access efficiency requirements of the system. See, e.g., Chapter 2 of Database System Concepts by Korth and Silberschatz.

The DAC **400** architecture uses a WEB based paradigm using an enhanced Domain Name Services (DNS), the Microsoft Component Object Model (DCOM), and Windows NT Application Program Interfaces (APIs) to facilitate communication and load balancing among the servers comprising the DAC server **402**. As is known to persons of ordinary skill in the art, DNS, which is also known as Bind, statically translates name requests to Internet Protocol 4 (IP4) addresses. In the DAC **400** architecture, an enhanced DNS dynamically assigns IP**4** addresses to balance the load among the servers comprising the DAC server **402**.

In the preferred embodiment, the enhanced DNS is designed and implemented using objects from Microsoft DCOM. Using the DCOM objects, the enhanced DNS acquires real-time server load performance statistics on each server comprising the DAC server **402** from the Windows NT API at set intervals. Based on these load performance statistics, the enhanced DNS adjusts the mapping of name requests to IP**4** addresses to direct data toward the servers which are more lightly loaded.

A large bank of modems **404** polls the DATs **200** at the customer sites within the DAC's **400** region. In the preferred embodiment, the bank of modems **404**, available as CISCO AS5200, is an aggregate **48** modem device with Local Area Network (LAN) **406** connectivity which permits the DAC servers **402** to dial the DATs **200** without requiring **48** separate modems and serial connections.

The DAC servers **402** and the bank of modems **404** are connected on a LAN **406**. In the preferred embodiment, the LAN uses a switched 100BaseT/10BaseT communication hardware layer protocol. As is known to persons of ordinary skill in the art, the 100BaseT/10BaseT protocol is based on the Ethernet model. Further, the numbers 100 and 10 refer to the communication link speed in megabits per second. In the preferred embodiment, the CISCO Catalyst 2900 Network Switch supports the LAN **406** connectivity between the devices connected to the LAN **406** including the DAC servers **402** and the bank of modems **404**.

As is known to persons of ordinary skill in the art, alternate LAN architectures could be used to facilitate communication among the devices of the LAN **406**. For example, the LAN **406** could use a hub architecture with a round robin allocation algorithm, a time division multiplexing algorithm or a statistical multiplexing algorithm.

A Wide Area Network (WAN) router **408** connects the LAN **406** to the WAN to facilitate communication between the DACs **400** and the DPCs **600**. In the preferred embodiment, the WAN router **408** is a CISCO 4700 WAN Router. The WAN router **408** uses frame relay connectivity to connect the DAC LAN **406** to the WAN. As is known to persons of ordinary skill in the art, alternate devices, such as the NORTEL Magellen Passport "50" Telecommunication Switch, could be used to facilitate communication between the DACs **400** and the DPCs **600** as long as the selected router meets the performance and quality communication requirements of the system.

As is known to persons of ordinary skill in the art, frame relay is an interface protocol for statistically multiplexed packet-switched data communications in which variable-sized packets (frames) are used that completely enclose the user packets which they transport. In contrast to dedicated point to point links that guarantee a specific data rate, frame relay communication provides bandwidth on-demand with a guaranteed minimum data rate. Frame relay communication also allows occasional short high data rate bursts according to network availability.

Each frame encloses one user packet and adds addressing and verification information. Frame relay data communication typically has transmission rates between 56 kilobytes per second (kb/s) and 1.544 megabytes per second (Mb/s). Frames may vary in length up to a design limit of approximately 1 kilobyte.

The Telco Carrier Cloud **412** is a communication network which receives the frames destined for the DPC **600** sent by the WAN router **408** from the DACs **400**. As is known to persons of ordinary skill in the art, carriers provide communication services at local central offices. These central offices contain networking facilities and equipment to inter-

connect telephone and data communications to other central offices within its own network and within networks of other carriers.

Since carriers share the component links of the interconnection network, data communication must be dynamically assigned to links in the network according to availability. Because of the dynamic nature of the data routing, the interconnection network is referred to as a carrier cloud of communication bandwidth.

All the DAC **400** equipment is on fully redundant on-line UPS power supplies to insure maximum power availability. Further, to minimize the time for trouble detection, trouble analysis and repair, all the DAC **400** equipment incorporates trouble detection and remote reporting/diagnostics as is known to an artisan of ordinary skill in the art.

FIG. **5** is a flow chart **500** describing the polling of the DATs **200** by a DAC **400** and the transmission of the TECBIs from the DATs **200** to the DAC **400**. In step **502**, the DAC server **402** reads the address of the first DAT **200** in its region for polling. In step **504**, a modem in the modem bank **404** dials the first DAT **200**. The DAC **400** determines whether the call to the DAT **200** was successful in step **506**. If the call to the first DAT **200** was unsuccessful, the DAC **400** will record the error condition in the session summary report and will report the error to the DPC **600** in step **522**.

If the call to the first DAT **200** was successful, the DAC **400** will verify that the DAT **200** is ready to transmit in step **508**. If the DAT **200** is not ready to transmit, the DAC **400** will record the error condition in the session summary report and will report the error to the DPC **600** in step **522**.

If the DAT **200** is ready to transmit in step **508**, the DAT **200** will transmit a TECBI packet header to the DAC **400** in step **510**. The DAC **400** will determine whether the transmission of the TECBI packet header was successful in step **512**. If the transmission of the TECBI packet header was unsuccessful, the DAC **400** will record the error condition in the session summary report and will report the error to the DPC **600** in step **522**.

If the transmission of the TECBI packet header was successful in step **512**, the DAT **200** will transmit a TECBI packet to the DAC **400** in step **514**. The DAC **400** will determine whether the transmission of the TECBI packet was successful in step **516**. If the transmission of the TECBI packet header was unsuccessful, the DAC **400** will record the error condition in the session summary report and will report the error to the DPC **600** in step **522**.

If the transmission of the TECBI packet was successful in step **516**, the DAC **400**, in step **518**, will compare the TECBI packet header transmitted in step **510** to the TECBI packet transmitted in step **514**. If the TECBI packet header does not match the TECBI packet, the DAC **400** will record the error condition in the session summary report and will report the error to the DPC **600** in step **522**.

If the TECBI packet header matched the TECBI packet in step **518**, the DAC **400** will set the status of the TECBI packet to indicate that it is ready for transmission to the DPC **600** in step **520**. The DAC **400** will also transmit the status to the DAT **200** to indicate successful completion of the polling and transmission session in step **520**. Next, the DAC **400** will determine whether TECBIs have been transmitted from all of the DATs **200** in its region in step **524**. If all DATs **200** in the DAC's **400** region have transmitted TECBIs to the DAC **400**, the DAC **400** will compile a DAT **200** status report in step **528** before terminating the session.

If one or more DATs **200** in the DAC's **400** region have not transmitted TECBIs to the DAC **400**, the DAC **400** will get the address of the next DAT **200** in the region in step **526**. Next, control returns to step **504** where the next DAT **200** in the DAC's **400** region will be polled as previously discussed.

In the preferred embodiment, the DAC server **402** initiates the polling and data transmission at optimum toll rate times to decrease the cost of data transmission. In addition to the raid drives and redundant servers, the DAC **400** will also have dual tape backup units which will periodically backup the entire data set. If there is a catastrophic failure of the DAC **400**, the tapes can be retrieved and sent directly to the DPC **600** for processing. As the DAT **200** polling and data transmission progresses, the DAC **400** will periodically update the DPC **600** with its status. If there is a catastrophic failure with the DAC **400**, the DPC **600** would know how much polling and backup has been done by the failing DAC **400**. Accordingly, the DPC **600** can easily assign another DAC **400** to complete the polling and data transmission for the DATs **200** in the failed DAC's **400** region.

FIG. **6** is a block diagram of the DPC **600** architecture. The DPC **600** accumulates, processes and stores images for later retrieval by DataTreasury™ System retrieval customers who have authorization to access relevant information. DataTreasury™ System retrieval customers include credit card merchants, credit card companies, credit information companies and consumers. As shown in FIG. **6** and FIG. **1**, the DPC **600** polls the DACs **400** and receives TECBIs which have accumulated in the DACs **400**.

In the preferred embodiment, the DPC server **602** comprises stand-alone Digital Equipment Corporation (DEC) SMP Alpha 4100 4/566 servers which are connected on a common network running Windows NT. The DEC Alpha servers manage the collection and intermediate storage of images and data which are received from the DACs **400**.

In the preferred embodiment, the DPC server **602** also comprises EMC **3700** SYMMETRIX CUBE Disk Storage Systems, which store the images and data collected and managed by the DEC Alpha servers. Like the DAC **400** architecture, the DPC **600** architecture uses a SYMMETRIX Remote Data Facility (SRDF), available from EMC, to enable multiple, physically separate data centers housing EMC Storage Systems to maintain redundant backups of each other across a Wide Area Network (WAN).

Like the DAC **400** architecture, the DPC **600** architecture uses a WEB based paradigm using an enhanced Domain Name Services (DNS), the Microsoft Component Object Model (DCOM), and Windows NT Application Program Interfaces (APIs) to facilitate communication and load balancing among the servers comprising the DPC server **602** as described above in the discussion of the DAC **400** architecture.

The workstation **604** performs operation control and system monitoring and management of the DPC **600** network. In the preferred embodiment, the workstation **604**, available from Compaq, is an Intel platform workstation running Microsoft Windows NT 4.x. The workstation **604** should be able to run Microsoft Windows NT 5.x when it becomes available. The workstation **604** executes CA Unicenter TNG software to perform network system monitoring and management. The workstation **604** executes SnoBound Imaging software to display and process TECBIs.

The workstation **604** also performs identification verification by comparing signature data retrieved remotely by the DATs **200** with signature data stored at the DPC **600**. In the preferred embodiment, signature verification software, available from Communications Intelligence Corporation of Redwood Shores, Calif. executing on the workstation **604**

performs the identification verification. As is known to persons of ordinary skill in the art, the workstation **604** could execute other software to perform identification verification by comparing biometric data including facial scans, fingerprints, retina scans, iris scans and hand geometry. Thus, the DPC **600** could verify the identity of a person who is making a purchase with a credit card by comparing the biometric data captured remotely with the biometric data stored at the DPC **600**.

As is known to persons of ordinary skill in the art, the DataTreasury™ System **100** could use workstations with central processing units from other integrated circuit vendors as long as the chosen workstation has the ability to perform standard operations such as fetching instructions, fetching data, executing the fetched instructions with the fetched data and storing results. Similarly, the DataTreasury™ System **100** could use alternate windows operating systems and network monitoring software as long as the selected software can monitor the status of the workstations and links in the network and display the determined status to the operator.

The Remote Data Entry Gateway **614** and the Remote Offsite Data Entry Facilities **616** correct errors which occurred during data capture by the DAT **200**. Since the DataTreasury™ System **100** partitions the document as described in the discussion of the sample receipt of FIG. **3***b*, the operator at the Remote Data Entry Gateway **614** or the Remote Offsite Date Entry Facilities **616** only needs to correct the portion of the document or image snippet which contained the error.

Partitioning improves system performance, decreases system cost and improves system quality. With partitioning, the DPC Server **602** only sends the portion of the document containing the error to the Remote Data Entry Gateway **614** or the Remote Offsite Data Entry Facilities **616**. Since the operator at these data entry locations only sees the portion of the document which contained the error, she can quickly recognize and correct the error. Without partitioning, the operator would have to search for the error in the entire document. With this inefficient process, the operator would need more time and would be more likely to make a mistake by missing the error or making a modification in the wrong location. Accordingly, partitioning improves system performance and quality by increasing the speed and accuracy of the error correction process.

Similarly, partitioning decreases the traffic on the DPC LAN **606** and the Telco Carrier Cloud **412** because the DPC Server **602** only sends the image snippet containing the error to the Remote Offsite Data Entry Facility **616** or the Remote Data Entry Gateway **614**. Accordingly, partitioning decreases system cost by reducing the bandwidth requirement on the interconnection networks.

A DPC LAN **606** facilitates communication among the devices which are connected to the LAN **606** including the DPC server **602** and the network workstation **604**. In the preferred embodiment, the DPC LAN **606** uses a switched 100BaseT/10BaseT communication hardware layer protocol like the DAC LAN **406** discussed earlier. In the preferred embodiment, the DPC LAN **406** is a high speed OC**2** network topology backbone supporting TCP/IP. The CISCO Catalyst 5500 Network Switch supports the DPC LAN **606** connectivity among the devices connected to the LAN **606**.

As is known to persons of ordinary skill in the art, alternate LAN architectures could be used to facilitate communication among the devices of the LAN **406**. For example, the LAN **406** could use a hub architecture with a round robin allocation algorithm, a time division multiplexing algorithm or a statistical multiplexing algorithm.

A Wide Area Network (WAN) router **612** connects the DPC LAN **606** to the WAN to facilitate communication between the DACs **400** and the DPCs **600**. In the preferred embodiment, the WAN router **612** is a CISCO 7507 WAN Router. The WAN router **612** uses frame relay connectivity to connect the DPC LAN **612** to the WAN. As is known to persons of ordinary skill in the art, alternate devices, such as the NORTEL Magellen Passport "50" Telecommunication Switch, could be used to facilitate communication between the DACs **400** and the DPCs **600** as long as the selected router meets the performance and quality communication requirements of the system

The DPC **600** has a three tier storage architecture to support the massive storage requirement on the DataTreasury™ System **100**. In the preferred embodiment, the storage architecture consists of Fiber Channel RAID technology based EMC Symmetrix Enterprise Storage Systems where individual cabinets support over 1 Terabyte of storage. After TECBI images have been processed and have been on-line for 30 days, they will be moved to DVD based jukebox systems. After the TECBI images have been on-line for 90 days, they will be moved to Write Once Read Many (WORM) based jukebox systems **608** for longer term storage of up to 3 years in accordance with customer requirements.

In an alternate embodiment, the DPC **600** is intended to also configure a High Density Read Only Memory (HD-ROM) when it becomes available from NORSAM Technologies, Los Alamos, N. Mex., into optical storage jukebox systems **610**, such as that which is available from Hewlett Packard, to replace the DVD components for increased storage capacity. The HD-ROM conforms to CD-ROM form factor metallic WORM disc. The HD-ROM currently has a very large storage capacity of over 320 giga bytes (320 GB) on a single platter and has an anticipated capacity of several terabytes (TB) on a single platter. The DPC **600** uses IBM and Philips technology to read from the HD-ROM and to write to the HD-ROM.

The DPC Alpha servers of the DPC server **602** insert images and data received from the DACs **400** into a single database which is stored on the Digital Storage Works Systems using a data manipulation language as is well known to persons of ordinary skill in the art. In the preferred embodiment, the database is the V8.0 Oracle relational database which was designed to support both data and image storage within a single repository.

As known to persons of ordinary skill in the art, a relational database consists of a collection of tables which have a unique name. See, e.g., Chapter Three of Database System Concepts by Korth and Silberschatz. A database schema is the logical design of the database. Each table in a relational database has attributes. A row in a table represents a relationship among a set of values for the attributes in the table. Each table has one or more superkeys. A superkey is a set of one or more attributes which uniquely identify a row in the table. A candidate key is a superkey for which no proper subset is also a superkey. A primary key is a candidate key selected by the database designer as the means to identify a row in a table.

As is well known to persons of ordinary skill in the art, the DataTreasury™ System **100** could use other database models available from other vendors including the entity relationship model as long as the selected database meets the storage and access efficiency requirements of the system. See, e.g., Chapter 2 of Database System Concepts by Korth and Silberschatz.

An exemplary DPC **600** basic schema consists of the tables listed below. Since the names of the attributes are

descriptive, they adequately define the attributes' contents. The primary keys in each table are identified with two asterisks (**). Numeric attributes which are unique for a particular value of a primary key are denoted with the suffix, "NO". Numeric attributes which are unique within the entire relational database are denoted with the suffix, "NUM".

I. CUSTOMER: This table describes the DataTreasury™ System customer.
- A. **CUSTOMER_ID
- B. COMPANY_NAME
- C. CONTACT
- D. CONTACT_TITLE
- E. ADDR1
- F. ADDR2
- G. CITY
- H. STATE_CODE
- I. ZIP_CODE
- J. COUNTRY_CODE
- K. VOX_PHONE
- L. FAX_PHONE
- M. CREATE_DATE

II. CUSTOMER_MAIL_TO: This table describes the mailing address of the DataTreasury™ System customer.
- A. **MAIL_TO_NO
- B. **CUST_ID
- C. CUSTOMER_NAME
- D. CONTACT
- E. CONTACT_TILE
- F. ADDR1
- G. ADDR2
- H. CITY
- I. STATE_CODE
- J. ZIP_CODE
- K. COUNTRY_CODE
- L. VOX_PHONE
- M. FAX_PHONE
- N. CREATE_DATE
- O. COMMENTS

III. CUSTOMER_DAT_SITE: This table describes the DAT location of the DataTreasury™ System customer.
- A. **DAT_SITE_NO
- B. **CUST_ID
- C. CUSTOMER_NAME
- D. CONTACT
- E. CONTACT_TILE
- F. ADDR1
- G. ADDR2
- H. CITY
- I. STATE_CODE
- J. ZIP_CODE
- K. COUNTRY_CODE
- L. VOX_PHONE
- M. FAX_PHONE
- N. CREATE_DATE
- O. COMMENTS

IV. CUSTOMER_SITE_DAT: This table describes the DAT site(s) of the DataTreasury™ System customer.
- A. **DAT_TERMINAL_ID
- B. **DAT_SITE_NO
- C. **CUST_ID
- D. INSTALL_DATE
- E. LAST_SERVICE_DATE
- F. CREATE_DATE
- G. COMMENTS

V. DATA_SPEC: This table provides data specifications for document partitioning and extraction.
- A. **DATA_SPEC_ID
- B. **CUST_ID
- C. DESCR
- D. RECORD_LAYOUT_RULES
- E. CREATE_DATE
- F. COMMENTS

VI. DATA_SPEC_FIELD: This table provides field data specifications for document partitioning and extraction.
- A. **DATA_SPEC_NO
- B. **DATA_SPEC_ID
- C. FIELD_NAME
- D. DESCR
- E. DATA_TYPE
- F. VALUE_MAX
- G. VALUE_MIN
- H. START_POS
- I. END_POS
- J. FIELD_LENGTH
- K. RULES
- L. CREATE_DATE
- M. COMMENTS

VII. TEMPL_DOC: This table specifies the partitioning of a predefined document.
- A. **TEMPL_DOC_NUM
- B. DATA_SPEC_ID
- C. DESCR
- D. RULES
- E. CREATE_DATE
- F. COMMENTS

VIII. TEMPL_FORM: This table defines the location of forms on a predefined document.
- A. **TEMPL_FORM_NO
- B. **TEMPL_DOC_NUM
- C. SIDES_PER_FORM
- D. MASTER_IMAGE_SIDE_A
- E. MASTER_IMAGE_SIDE_B
- F. DISPLAY_ROTATION_A
- G. DISPLAY_ROTATION_B
- H. DESCR
- I. RULES
- J. CREATE_DATE

IX. TEMPL_PANEL: This table specifies the location of panels within the forms of a predefined document.
- A. **TEMPL_PANEL_NO
- B. **TEMPL_SIDE_NO
- C. **TEMPL_FORM_NO
- D. **TEMPL_DOC_NUM
- E. DISPLAY_ROTATION
- F. PANEL_UL_X
- G. PANEL_UL_Y
- H. PANEL_LR_X

I. PANEL_LR_Y

J. DESCR

K. RULES

L. CREATE_DATE

X. TEMPL_FIELD: This table defines the location of fields within the panels of a form of a predefined document.

A. **TEMPL_FIELD_NO

B. **TEMPL_PANEL_NO

C. **TEMPL_SIDE_NO

D. **TEMPL_FORM_NO

E. **TEMPL_DOC_NUM

F. DISPLAY_ROTATION

G. FLD_UL_X

H. FLD_UL_Y

I. FLD_LR_X

J. FLD_LR_Y

K. DESCR

L. RULES

M. CREATE_DATE

XI. DAT_BATCH: This table defines batches of documents which were processed during a DAT session.

A. **DAT_BATCH_NO

B. **DAT_SESSION_NO

C. **DAT_SESSION_DATE

D. **DAT_TERMINAL_ID

E. DAT_UNIT_CNT

F. CREATE_DATE

XII. DAT_UNIT: This table defines the unit in a batch of documents which were processed in a DAT session.

A. **DAT_UNIT_NUM

B. **DAT_BATCH_NO

C. **DAT_SESSION_NO

D. **DAT_SESSION_DATE

E. **DAT_TERMINAL_ID

F. FORM_CNT

G. DOC_CNT

H. CREATE_DATE

XIII. DAT_DOC: This table defines documents in the unit of documents which were processed in a DAT session.

A. **DAT_DOC_NO

B. **DAT_UNIT_NUM

C. DOC_RECORD_DATA

D. CREATE_DATE

The DATA_SPEC, DATA_SPEC_FIELD, TEMPL_DOC, TEMPL_FORM, TEMPL_PANEL and TEMPL_FIELD tables implement the document partitioning algorithm mentioned above in the discussion of the sample receipt of FIG. **3***b*. The cross product of the DATA_SPEC and DATA_SPEC_FIELD tables partition arbitrary documents while the cross product of the TEMPL_DOC, TEMPL_FORM, TEMPL_PANEL and TEMPL_FIELD tables partition predefined documents of the DataTreasury™ System **100**. The TEMPL-FORM defines the location of forms on a predefined document. The TEMPL-PANEL defines the location of panels within the forms of a predefined document. Finally, the TEMPL_FIELD table defines the location of fields within the panels of a form of a predefined document.

The DPC **600** performs data mining and report generation for a wide variety of applications by returning information from the data base. For example, the DPC **600** generates market trend analysis reports and inventory reports for merchants by analyzing the data from receipts captured by the DAT **200**. The DPC **600** also can provide important tax information to the taxpayer in the form of a report or to software applications like tax preparation software by retrieving tax information from the database which originally resided on receipts, documents and electronic transactions captured by the DAT **200**. Similarly, the DPC **600** can also provide tax information for particular periods of time for a tax audit.

FIG. **7** is a flow chart **700** describing the polling of the DACs **300** by a DPC **600** and the transmission of the TECBIs from the DACs **300** to the DPC **600**. In step **702**, the DPC **600** reads the address of the first DAC **300** in its region for polling. In step **704**, the DPC **600** connects with a DAC **300** for transmission. The DPC **600** determines whether the connection to the DAC **300** was successful in step **706**. If the call to the DAC **300** was unsuccessful, the DPC **600** will record the error condition in the session summary report and will report the error to the DPC **600** manager in step **722**.

If the connection to the DAC **300** was successful, the DPC **600** will verify that the DAC **300** is ready to transmit in step **708**. If the DAC **300** is not ready to transmit, the DPC **600** will record the error condition in the session summary report and will report the error to the DPC **600** manager in step **722**.

If the DAC **300** is ready to transmit in step **708**, the DAC **300** will transmit a TECBI packet header to the DPC **600** in step **710**. The DPC **600** will determine whether the transmission of the TECBI packet header was successful in step **712**. If the transmission of the TECBI packet header was unsuccessful, the DPC **600** will record the error condition in the session summary report and will report the error to the DPC **600** manager in step **722**.

If the transmission of the TECBI packet header was successful in step **712**, the DAC **300** will transmit a TECBI packet to the DPC **600** in step **714**. The DPC **600** will determine whether the transmission of the TECBI packet was successful in step **716**. If the transmission of the TECBI packet header was unsuccessful, the DPC **600** will record the error condition in the session summary report and will report the error to the DPC **600** manager in step **722**.

If the transmission of the TECBI packet was successful in step **716**, the DPC **600**, in step **718**, will compare the TECBI packet header transmitted in step **710** to the TECBI packet transmitted in step **714**. If the TECBI packet header does not match the TECBI packet, the DPC **600** will record the error condition in the session summary report and will report the error to the DPC **600** manager in step **722**.

If the TECBI packet header matched the TECBI packet in step **718**, the DPC **600** will set the status of the TECBI packet to indicate that it was received at the DPC **600** in step **720**. The DPC **600** will also transmit the status to the DAC **300** to indicate successful completion of the polling and transmission session in step **720**. Next, the DPC **600** will determine whether TECBIs have been transmitted from all of the DACs **300** in its region in step **724**. If all DACs **300** in the DPC's **600** region have transmitted TECBIs to the DPC **600**, the DPC **600** will compile a DAC **300** status report in step **728** before terminating the session.

If one or more DACs **300** in the DPC's **600** region have not transmitted TECBIs to the DPC **600**, the DPC **600** will get the address of the next DAC **300** in the region in step **726**. Next, control returns to step **704** where the next DAC **300** in the DPC's **600** region will be polled as previously discussed.

FIG. **8** is a flow chart **800** describing the data processing performed by the DPC **600**. In step **802**, the DPC **600** fetches

the first TECBI packet. Next, the DPC **600** extracts the first TECBI from the TECBI packet in step **804**. In step **806**, the DPC **600** inserts the TECBI into the database. In step **808**, the DPC **600** extracts the tag header which includes the customer identifier, the encryption keys and the template identifier from the TECBI to obtain the ECBI.

In step **810**, the DPC **600** decrypts the ECBI image to obtain the CBI. In step **812**, the DPC **600** uncompresses the CBI to obtain the BI. In step **814**, the DPC **600** fetches and applies the BI template against the BI. Further the DPC **600** divides the BI into image snippets and tags the BI template with data capture rules in step **814** to form the Tagged Bitmap Image Snippets (TBIS). In step **816**, the DPC **600** submits the TBISs for data capture operations to form the IS Derived Data Record (ISDATA). The DPC **600** discards the TBISs upon completion of the data capture operations in step **816**. In step **818**, the DPC **600** updates the TECBI record in the database with the IS Derived Data.

In step **820**, the DPC **600** determines whether it has processed the last TECBI in the TECBI packet. If the last TECBI in the TECBI packet has not been processed, the DPC **600** extracts the next TECBI from the TECBI packet in step **822**. Next, control returns to step **806** where the next TECBI will be processed as described above.

If the last TECBI in the TECBI packet has been processed, the DPC **600** determines whether the last TECBI packet has been processed in step **824**. If the last TECBI packet has not been processed, the DPC **600** fetches the next TECBI packet in step **826**. Next, control returns to step **804** where the next TECBI packet will be processed as described above. If the last TECBI packet has been processed in step **824**, the DPC **600** terminates data processing.

As is known to persons of ordinary skill in the art, a user can request information from a relational database using a query language. See, e.g., Chapter Three of Database System Concepts by Korth and Silberschatz. For example, a user can retrieve all rows of a database table having a primary key with particular values by specifying the desired primary key's values and the table name on a select operation. Similarly, a user can retrieve all rows from multiple database tables having primary keys with particular values by specifying the desired primary keys' values and the tables with a select operation.

The DataTreasury™ System provides a simplified interface to its retrieval customers to enable data extraction from its relational database as described in FIG. **9**. For example, a DataTreasury™ System customer can retrieve the time, date, location and amount of a specified transaction.

The DPC **600** performs data mining and report generation for a wide variety of applications by returning information from the data base. For example, the DPC **600** generates market trend analysis reports and inventory reports for merchants by analyzing the data from receipts captured by the DAT **200**. The DPC **600** also can provide important tax information to the taxpayer in the form of a report or to tax preparation software by retrieving tax information from the database which originally resided on receipts, documents and electronic transactions captured by the DAT **200**. Similarly, the DPC **600** can also provide tax information for particular periods of time for a tax audit.

FIG. **9** is a flowchart **900** describing the data retrieval performed by the DPC **600**. In step **902**, the DPC **600** receives a TECBI retrieval request. In step **904**, the DPC **600** obtains the customer identifier. In step **906**, the DPC **600** determines whether the customer identifier is valid. If the customer identifier is not valid, control returns to step **904** where the DPC **600** will obtain another customer identifier.

If the customer identifier is valid in step **906**, the DPC **600** will obtain the customer security profile in step **908**. In step **910**, the DPC **600** receives a customer retrieval request. In step **912**, the DPC **600** determines whether the customer retrieval request is consistent with the customer security profile. If the customer retrieval request is not consistent with the customer security profile, control returns to step **910** where the DPC **600** will obtain another customer retrieval request. If the customer retrieval request is consistent with the customer security profile, the DPC **600** will transmit the results to the customer as indicated by the customer security profile in step **914**.

While the above invention has been described with reference to certain preferred embodiments, the scope of the present invention is not limited to these embodiments. One skilled in the art may find variations of these preferred embodiments which, nevertheless, fall within the spirit of the present invention, whose scope is defined by the claims set forth below.

What is claimed is:

1. A system for central management, storage and report generation of remotely captured paper transactions from documents and receipts comprising:

one or more remote data access subsystems for capturing and sending paper transaction data and subsystem identification information comprising at least one imaging subsystem for capturing the documents and receipts and at least one data access controller for managing the capturing and sending of the transaction data;

at least one central data processing subsystem for processing, sending, verifying and storing the paper transaction data and the subsystem identification information comprising a management subsystem for managing the processing, sending and storing of the of the transaction data; and

at least one communication network for the transmission of the transaction data within and between said one or more data access subsystems and said at least one data processing subsystem, with the data access subsystem providing encrypted subsystem identification information and encrypted paper transaction data to the data processing subsystem.

2. A system as in claim **1** wherein said one or more data access subsystems further comprise at least one scanner for capturing the paper transaction data.

3. A system as in claim **2** wherein said one or more data access subsystems also capture electronic transactions from credit cards, smart cards and debit cards, signature data or biometric data, further comprising:

at least one card interface for capturing the electronic transaction data;

at least one signature interface for capturing an electronic signature; and

at least one biometric interface for capturing biometric data.

4. A system as in claim **3** wherein said at least one data access controller successively transforms the captured transaction data to a bitmap image, a compressed bitmap image, an encrypted, compressed bitmap image and an encrypted, compressed bitmap image tagged with information identifying a location and time of the transaction data capture.

5. A system as in claim **4** wherein said one or more data access subsystems further comprise digital storage for storing the tagged, encrypted, compressed bitmap image.

6. A system as in claim **5** wherein said at least one card interface initiates the electronic transaction.

7. A system as in claim 6 wherein said one or more data access subsystems further comprise at least one printer for printing the paper transaction initiated by said at least one card interface.

8. A system as in claim 7 wherein the paper transaction printed by said at least one printer includes data glyphs.

9. A system as in claim 1 wherein said data management subsystem of said at least one data processing subsystem comprises:

at least one server for polling said one or more remote data access subsystems for transaction data;

a database subsystem for storing the transaction data in a useful form;

a report generator for generating reports from the transaction data and providing data to software applications;

at least one central processing unit for managing the storing of the transaction data;

a domain name services program for dynamically assigning one of said at least one server to receive portions of the transaction data for balancing the transaction data among said at least one server; and

a memory hierarchy.

10. A system as in claim 9 wherein said at least one server also polls for biometric and signature data, said database stores the biometric data and the signature data, and said at least one central processing unit verifies the biometric data and the signature data.

11. A system as in claim 9 wherein said memory hierarchy comprises at least one primary memory for storage of recently accessed transaction data and at least one secondary memory for storage of other transaction data.

12. A system as in claim 11 wherein said at least one secondary memory comprises at least one write once read many jukebox and at least one optical storage jukebox.

13. A system as in claim 12 wherein said at least one optical storage jukebox comprises read only memory technology including compact disc read only memory form factor metallic write once read many disc.

14. A system as in claim 9 wherein said database subsystem comprises at least one predefined template for partitioning the stored transaction data into panels and identifying locations of the panels.

15. A system as in claim 14 wherein said data processing subsystem further comprises a data entry gateway for correcting errors in the panels of stored transaction data.

16. A system as in claim 1 wherein said at least one communication network comprises:

at least one first local area network for transmitting data within a corresponding one of said one or more remote data access subsystems;

at least one second local area network for transmitting data within a corresponding one of said at least one data processing subsystem; and

at least one wide area network for transmitting data between said one or more remote data access subsystems and said at least one data processing subsystem.

17. A system as in claim 16 wherein said at least one communication network further comprises:

at least one modem for connecting said at least one first local area network of said one or more data access subsystems to a corresponding one of said at least one second local area network of said at least one data processing subsystem through said at least one wide area network; and

at least one bank of modems for connecting said at least one second local area network of said at least one data processing subsystem to a corresponding some of said at least one first local area network of said one or more data access subsystems through said at least one wide area network.

18. A system as in claim 1 further comprising at least one data collecting subsystem for collecting and sending the electronic or paper transaction data comprising a further management subsystem for managing the collecting and sending of the transaction data.

19. A system as in claim 18 wherein said further data management subsystem of said at least one data collecting subsystem comprises:

at least one server for polling said one or more remote data access subsystems for transaction data;

a database for storing the transaction data in a useful form;

at least one central processing unit for managing the collecting of the transaction data;

a domain name services program for dynamically assigning one of said at least one server to receive portions of the transaction data for balancing the transaction data among said at least one server; and

a memory hierarchy.

20. A system as in claim 19 wherein said memory hierarchy comprises at least one primary memory for collecting transaction data and at least one secondary memory for backup storage of the transaction data.

21. A system as in claim 20 wherein said at least one secondary memory comprises at least one DLT jukebox.

22. A system as in claim 18 wherein said at least one communication network comprises:

at least one first local area network for transmitting data within a corresponding one of said one or more remote data access subsystems;

at least one second local area network for transmitting data within a corresponding one of said at least one data collection subsystem;

at least one third local area network for transmitting data within a corresponding one of said at least one data processing subsystem; and

at least one wide area network for transmitting data between said one or more remote data access subsystems, said at least one data collection subsystem and said at least one data processing subsystem.

23. A system as in claim 22 wherein said at least one communication network further comprises:

at least one first modem for connecting said at least one first local area network of said one or more data access subsystems to a corresponding one of said at least one second local area network through said at least one wide area network;

at least one bank of modems for connecting said at least one second local area network of said at least one data collection subsystem to a corresponding some of said at least one first local area network of said one or more data access subsystems through said at least one wide area network;

at least one first wide area network router for connecting a corresponding one of said at least one second local area network of said at least one data collecting subsystem to said at least one wide area network; and

at least one second wide area network router for connecting a corresponding one of said at least one third local area network of said at least one data processing subsystem to said at least one wide area network.

24. A system as in claim 23 wherein said at least one first wide area network and said at least one second wide area network comprises a carrier cloud, said carrier cloud using a frame relay method for transmitting the transaction data.

25. A system as in claim 22 wherein said at least one second local area network and said at least one third local area network further comprises a corresponding one of at least one network switch for routing transaction data within said at least one second local area network and said at least one third local area network.

26. A method for central management, storage and verification of remotely captured paper transactions from documents and receipts comprising the steps of:

capturing an image of the paper transaction data at one or more remote locations and sending a captured image of the paper transaction data;

managing the capturing and sending of the transaction data;

collecting, processing, sending and storing the transaction data at a central location;

managing the collecting, processing, sending and storing of the transaction data;

encrypting subsystem identification information and the transaction data; and

transmitting the transaction data and the subsystem identification information within and between the remote location(s) and the central location.

27. The method as in claim 26 wherein said managing the capturing and sending step comprises the steps of:

successively transforming the captured transaction data to a bitmap image, a compressed bitmap image, an encrypted, compressed bitmap image and an encrypted, compressed bitmap image tagged with information identifying a location and time of the transaction data capturing; and

storing the tagged, encrypted, compressed bitmap image.

28. The method as in claim 27 wherein said managing the capturing and sending step also captures electronic transactions from credit cards, smart cards and debit cards, signature data or biometric data, further comprising the steps of:

initiating an electronic transaction;

capturing signature data;

capturing biometric data; and

printing a paper transaction with data glyphs for the initiated electronic transaction.

29. A method as in claim 26 wherein:

said capturing and sending step occurs at a plurality of remote locations; and

said collecting, processing, sending and storing step occurs at a plurality of central locations.

30. A method as in claim 29 wherein said collecting, processing, sending and storing step comprises the steps of:

polling the remote locations for transaction data with servers at the central locations;

storing the transaction data at the central location in a memory hierarchy, said storing maintains recently accessed transaction data in a primary memory and other transaction data in a secondary memory; and

dynamically assigning the servers at the central location to receive portions of the transaction data for balancing the transaction data among the servers; and

generating reports from the transaction data and providing data to software applications.

31. A method as in claim 30 wherein said storing the transaction data step comprises the steps of:

partitioning the stored transaction data with predefined templates into panels; and

identifying locations of the panels.

32. A method as in claim 31 wherein said managing the collecting, processing, sending and storing of the transaction data step comprises correcting errors in the panels of stored transaction data.

33. A method as in claim 32 further comprising the steps of:

polling the remote locations for captured electronic data, captured signature data and captured biometric data with servers at the central locations; and

comparing the captured signature data and the captured biometric data to stored signature data and stored biometric data respectively for identification verification.

34. A method as in claim 32 wherein said transmitting the transaction data step comprises the steps of:

transmitting data within the remote locations;

transmitting data from each remote location to a corresponding central location; and

transmitting data within the central locations.

35. A method as in claim 34 wherein said transmitting data from each remote location to a corresponding central location step comprises the steps of:

connecting each remote location to a corresponding central location; and

connecting each central location to corresponding remote locations.

36. A method as in claim 29 further comprising the steps of:

collecting and sending the electronic or paper transaction data at intermediate locations;

managing the collecting and sending of the transaction data; and

transmitting the transaction data within the intermediate location and between the intermediate locations and the remote locations and the central locations.

37. A method as in claim 36 wherein said managing the collecting and sending step comprises the steps of:

polling the remote locations for transaction data with servers in the intermediate locations;

storing the transaction data in the intermediate locations in a useful form, said storing maintains the transaction data in a primary memory of a memory hierarchy and performs backup storage of the transaction data into a secondary memory of the memory hierarchy; and

dynamically assigning the servers to receive portions of the transaction data for balancing the transaction data among the servers.

38. The method as in claim 36 wherein said transmitting the transaction data step comprises the steps of:

transmitting data within the remote locations;

transmitting data from each remote location to a corresponding intermediate location;

transmitting data within the intermediate locations;

transmitting data from each intermediate location to corresponding central locations; and

transmitting data within the central locations.

39. A method as in claim 38 wherein said transmitting data from each remote location to corresponding intermediate locations step comprises the steps of:

connecting each remote location to a corresponding intermediate location; and

connecting the intermediate locations to corresponding remote locations.

40. A method as in claim **38** wherein said transmitting data from each intermediate location to corresponding central locations comprises the steps of:

connecting each intermediate location to an external communication network; and

connecting the corresponding central locations to the communication network.

41. A method as in claim **40** wherein said transmitting data from each intermediate location to corresponding central locations step further comprises the steps of:

packaging the transaction data into frames; and

transmitting the frames through the external communication network.

42. A communication network for the transmission of data within and between one or more remote data processing subsystems, at least one intermediate data collecting subsystem and at least one central subsystem forming a tiered architecture wherein each of said at least one central data processing subsystem communicate with a corresponding some of said at least one data collecting subsystem and each of said at least one data collecting subsystem communicate with a corresponding some of said one or more data processing subsystems, said data processing subsystem including an imaging subsystem for capturing images of documents and receipts, comprising:

at least one first local area network for transmitting data within a corresponding one of said one or more remote subsystems;

at least one second local area network for transmitting data within a corresponding one of said at least one intermediate subsystem;

at least one third local area network for transmitting data within a corresponding one of said at least one central subsystem; and

at least one wide area network for transmitting data between said one or more remote subsystems, said at least one intermediate subsystem and said at least one central subsystem.

43. A communication network as in claim **42** further comprising:

at least one first modem for connecting said at least one first local area network of said one or more remote subsystems to a corresponding one of said at least one second local area network through said at least one wide area network;

at least one bank of modems for connecting said at least one second local area network of said at least one intermediate subsystem to a corresponding some of said at least one first local area network of said one or more remote subsystems through said at least one wide area network;

at least one first wide area network router for connecting a corresponding one of said at least one second local area network of said at least one intermediate subsystem to said at least one wide area network; and

at least one second wide area network router for connecting a corresponding one of said at least one third local area network of said at least one central subsystem to said at least one wide area network.

44. A system as in claim **43** wherein said at least one first wide area network and said at least one second wide area network comprises a carrier cloud which utilizes a frame relay method for transmitting the transaction data.

45. A system as in claim **44** wherein said at least one second local area network and said at least one third local area network further comprises a corresponding one of at least one network switch for routing transaction data within said at least one second local area network and said at least one third local area network; and further wherein said data comprises (a) electronic transactions from credit cards, smart cards and debit cards, signature data or biometric data, or (b) paper transactions from documents and receipts.

46. A method for transmitting data within and between one or more remote subsystems, at least one intermediate subsystem and at least one central subsystem in a tiered manner wherein each of the central subsystems communicate with at least one intermediate subsystem and each of the intermediate subsystems communicate with at least one remote subsystems comprising the steps of:

capturing an image of documents and receipts and extracting data therefrom;

transmitting data within the remote locations;

transmitting data from each remote location to corresponding intermediate location;

transmitting data within the intermediate locations;

transmitting data from each intermediate location to corresponding central locations; and

transmitting data within the central locations.

47. A method as in claim **46** wherein said transmitting data from each remote location to corresponding intermediate locations step comprises the steps of:

connecting each remote location to a corresponding intermediate location; and

connecting the intermediate locations to corresponding remote locations.

48. A method as in claim **47** wherein said transmitting data from each intermediate location to corresponding central locations comprises the steps of:

connecting each intermediate location to an external communication network; and

connecting the corresponding central locations to the external communication network.

49. A method as in claim **48** wherein said transmitting data from each intermediate location to corresponding central locations step further comprises the steps of:

packaging the transaction data into frames; and

transmitting the frames through the external communication network.

50. A method as in claim **46** wherein said data is obtained from (a) electronic transactions from credit cards, smart cards and debit cards, signature data or biometric data, or (b) paper transactions from documents and receipts.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : **5,910,988**

DATED : **June 8, 1999**

INVENTOR(S) : **Claudio R. Ballard**

It is certified that error appears in the above-indentified patent and that said Letters Patent is hereby corrected as shown below:

On the title page: item **(56) References Cited Delete "4,602,936" and insert –5,602,936–.**
On the title page: Abstract Delete"Locations" after the words more remote and insert -- locations **--.**

Column 4, **Line 26: Delete "(DACS)" after the word Collectors and insert –(DACs)–.**
Column 9, **Line 35: Delete "3i band" after the word in FIG. and insert –3b and–.**
Column 28, **Line 23: Delete "subsystems" after the word remote and insert –subsystem–.**

Signed and Sealed this

Twelfth Day of October, 1999

Attest:

Q. TODD DICKINSON

Attesting Officer

Acting Commissioner of Patents and Trademarks

U.S. DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

October 6, 2015
(Date)

THIS IS TO CERTIFY that the attached document is a list of the papers that comprise the record before the Patent Trial and Appeal Board (PTAB) for the *Covered Business Method Patent Review* proceeding identified below:

FIDELITY NATIONAL INFORMATION SERVICES,
Petitioner
v.

DATATREASURY CORP.,
Patent Owner

Case: CBM2014-00021
Patent 5,910,988

By authority of the

DIRECTOR OF THE UNITED STATES PATENT AND TRADEMARK OFFICE

Marcia L. Fletcher

Certifying Officer

Prosecution History CBM2014-00021

Date	Document
10/25/2013	Petition for Covered Business Method Patent Review
10/25/2013	Petitioner's Power of Attorney
11/15/2013	Notice of Filing Date Accorded to Petition
11/15/2013	Patent Owner's Mandatory Notices
1/17/2014	Petitioner's Supplemental Mandatory Notices
1/31/2014	Patent Owner's Preliminary Response
2/24/2014	Patent Owner's Updated Mandatory Notices
2/24/2014	Patent Owner's Submission of Corrected Exhibits
2/25/2014	Petitioner's Submission of Claim Scope Statement
2/25/2014	Petitioner's Exhibit List
3/26/2014	Petitioner's Second Supplemental Mandatory Notices
4/25/2014	Petitioner's Second Submission of Claim Scope Statement
4/29/2014	Decision - Institution of Covered Business Method Patent Review
4/29/2014	Scheduling Order
5/12/2014	Petitioner's Request for Rehearing
5/27/2014	Petitioner's List of Proposed Motions
5/27/2014	Patent Owner's List of Proposed Motions
6/2/2014	Petitioner's Request for Expedited Determination of Patentability
6/2/2014	Petitioner's Exhibit List
6/10/2014	Patent Owner's Opposition to Request for Expedited Determination
6/13/2014	Decision - Request for Rehearing
6/23/2014	Order - Conduct of the Proceedings
7/11/2014	Decision - Conduct of the Proceedings
7/29/2014	Patent Owner's Response
8/29/2014	Petitioner's Reply Brief
10/10/2014	Petitioner's Request for Oral Hearing
10/14/2014	Patent Owner's Request for Oral Argument
11/10/2014	Order - Trial Hearing
12/5/2014	Petitioner's Updated Exhibit List
12/5/2014	Patent Owner's Notification of Participation
12/5/2014	Patent Owner's Objection and Motion to Exclude
12/8/2014	Patent Owner's Withdrawal of Motion to Exclude
4/29/2015	Final Written Decision
5/29/2015	Patent Owner's Request for Rehearing
5/29/2015	Patent Owner's Updated Mandatory Notice
5/29/2015	Patent Owner's Appointment of Backup Counsel
6/26/2015	Decision - Request for Rehearing

United States Court of Appeals
for the Federal Circuit

DataTreasury Corporation v. Fidelity National Information, 2016-1046, -1048

CERTIFICATE OF SERVICE

I, Christian Hurt, being duly sworn according to law and being over the age of 18, upon my oath depose and say that:

On **January 6, 2016**, I electronically filed the foregoing **BRIEF OF THE APPELLANT** with the Clerk of Court using the CM/ECF System, which will serve via e-mail notice of such filing to all counsel registered as CM/ECF users, including any of the following:

Erika Arner
(Principal Counsel)
Finnegan, Henderson, Farabow,
Garrett & Dunner, LLP
Two Freedom Square
11955 Freedom Drive
Reston, VA 20190
erika.arner@finnegan.com
571-203-2700

Rachel L. Emsley
Finnegan, Henderson, Farabow,
Garrett & Dunner, LLP
Two Seaport Lane
6th Floor
Boston, MA 02210
rachel.emsley@finnegan.com
617-452-1600

Kevin D. Rodkey
Finnegan, Henderson, Farabow,
Garrett & Dunner, LLP
303 Peachtree Street, NE
3500 SunTrust Plaza
Atlanta, GA 30308
kevin.rodkey@finnegan.com
404-653-6400

Deborah G. Segers
Fidelity National Information
Systems, Inc.
601 Riverside Avenue
Tower, 12th Floor
Jacksonville, FL 32204
debbie.segers@fisglobal.com
414-357-2209

Paper copies will also be mailed to the above principal counsel at the time paper copies are sent to the Court.

Upon acceptance by the Court of the e-filed document, six paper copies will be filed with the Court within the time provided in the Court's rules.

January 6, 2016

/s/ Christian Hurt
Counsel for Appellant

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B), because it contains 10,402, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii) and Federal Circuit Rule 32(b).

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6), because it has been prepared in a proportionally spaced typeface using Microsoft Word 2011 for Mac in Times New Roman 14 point font.

Date: January 6, 2015

/s/ Christian Hurt

Christian Hurt
Attorney for Appellant